Università di Pisa

SCUOLA DI DOTTORATO IN

GIUSTIZIA COSTITUZIONALE E DIRITTI FONDAMENTALI

Dottorato di ricerca – XXII ciclo (2007-2010)

Direttore:

Chiar.mo Prof. Roberto Romboli

TUTELA DEI DIRITTI NELLA SOCIETA' GLOBALE:

RIFLESSIONI SUL RAPPORTO FRA *PRIVACY* E NUOVE TECNOLOGIE

Candidata: *Emanuela Brugiotti*

Relatore: *Chiar.mo Prof. Roberto Romboli*

Alla mia famiglia

"(...) la nostra Costituzione è in parte una realtà, ma soltanto in parte è una realtà. In parte è ancora un programma, un ideale, una speranza, un impegno di lavoro da compiere. Quanto lavoro avete da compiere! Quanto lavoro vi sta dinanzi!"
Dal *Discorso sulla Costituzione* di Pietro Calamandrei (26 gennaio 1955)

Indice

PREMESSA

La privacy, com'è stato giustamente osservato, rappresenta oggi una delle parole chiave per penetrare le riorganizzazioni delle società nell'epoca della globalizzazione e dell'informazione, nonché "la base su cui ciascuno di noi edifica liberamente la propria personalità" [1].

Le nuove dimensioni della raccolta e del trattamento delle informazioni personali, la pervasività del controllo sulle persone che oggi è possibile operare, da parte di soggetti sia pubblici che privati, ha provocato la moltiplicazione della richiesta di tutela e la consapevolezza dell'impossibilità di circoscrivere le relative problematiche nel quadro tradizionale, identificato originariamente da quel concetto.

Oggi, infatti, il centro di gravità è sempre più individuato, più che nel diritto ad essere lasciati soli, nella possibilità di ciascuno di noi di controllare l'uso delle informazioni che lo riguardano e nel considerare i problemi della privacy "nel quadro dell'attuale organizzazione del potere, di cui appunto l'infrastruttura informativa rappresenta ormai una della componenti fondamentali"[2].

In questo modo, la tecnologia sembra destinata a cambiare sempre più gli assetti istituzionali conosciuti e gli stessi processi democratici sono profondamente influenzati dal modo in cui circolano le informazioni[3].

Davanti alle enormi e ancora sconosciute possibilità che le nuove tecnologie pongono davanti ai nostri occhi, ci sono, quindi, anche i rischi connessi ad uno sviluppo fuori controllo, dovuto alla difficoltà della progettazione politica e normativa a tenere il passo.

L'esperienza giuridica non poteva non essere attraversata da queste nuove tensioni. Di fronte all'esigenza sempre più avvertita di norme giuridiche chiare e coerenti, condivise ed efficaci[4], ci si trova spesso di fronte ad un vero e proprio "disorientamento giuridico", in cui le stesse categorie tradizionali (dignità della persona, autodeterminazione

---

[1] S. RODOTà, *Intervista su privacy e libertà*, a cura di P. CONTI, Editori Laterza 2005.

[2] S. RODOTà, *Tecnologia e diritti*, Il Mulino, Bologna, 1995, pag 19.

[3] T. E. FROSINI, *Tecnologie e libertà costituzionali*, G. COMANDE' e G. PONZALLI(a cura di) in Scienza e diritto nel prisma del diritto comparato, Giuffrè, Milano, 2004, pag 189; S. RODOTà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazioni*, Laterza, Roma-Bari 1997.

[4] C. CASONATO, *Bioetica e pluralismo nello Stato Costituzionale*, consultabile in www.forumcostituzionale.it

individuale, diritto alla salute ecc) subiscono un effetto di spiazzamento e riformulazione.

Il concetto di privacy, così sfuggente ad ogni definizione che possa dirsi completamente esaustiva[5], viene sempre più accostato al valore persona[6], come mezzo per tutelare la sua dignità e il suo sviluppo all'interno della società.

Conferma di ciò si ha, per esempio, nell'esplicito richiamo al concetto di dignità presente nel nuovo Codice della privacy, concetto che, pertanto, è considerato il vero "nocciolo duro" della tutela offerta all'interessato a fronte dell'attività di trattamento dei dati personali[7], nonché uno dei suoi valori fondativi più preganti, in quanto principio che investe tutti gli aspetti della vita umana.

Si individua, così, un'altra caratteristica della privacy, ovvero la sua trasversalità.

Non stupisce, quindi, che la stessa dignità sia anche uno dei parametri più adoperati dalla giurisprudenza e dal Garante per la protezione dei dati personali, per delimitare l'area degli interessi rilevanti in materia di tutela del diritto alla privacy, diritto quanto mai complesso in cui coesistono, come si vedrà in seguito, aspetti diversi[8].

Senza contare che la società globale e l'incessante sviluppo delle nuove tecnologie, pongono sempre più alla nostra attenzione la transnazionalità

[5] C. DE GIACOMO, *Diritto, libertà e Privacy nel mondo della comunicazione globale*, Giuffrè, Milano, 1999, pag. 16 definisce la privacy come una "nozione ombrello, che sottende il riferimento ad una pluralità di interessi ed ambiti di vulnerabilità ben distinti ed individuabili" ; T. M. UBERTAZZI, *Diritto alla privacy, natura e funzioni giuridiche*, Cedam, Padova, 2004, pag 76, parla della concezione multidimensionale della privacy. D'altronde già lo stesso giudice Brandeis, nel famoso *dissent* nel caso Olmstead v. United States (277 U.S. 438), definiva la privacy come il più comprensivo dei diritti e Alan Westin, professore di Diritto Pubblico presso la Columbia University di New York, considerato uno dei maggiori esperti di privacy negli Stati Uniti, apriva il primo capitolo del suo libro *Privacy and Freedom* ammettendo la particolare difficoltà di autori e studiosi a mettersi d'accordo su un'unica definizione da attribuire al valore di privacy, A. F. WESTIN, *Privacy and Freedom*, Atheneum, New York, 1967, pag. 1.

[6] "Le moderne Costituzioni individuano nel principio personalistico il valore base da tutelare, nei confronti del quale le codificazioni dei singoli diritti rappresentano una specificazione storica delle posizioni soggettive che meritano un particolare riconoscimento. Le carte costituzionali si premurano, in altri termini, di costruire attorno alla persona umana considerata nella sua integrità, un complesso mosaico di diritti", così G. ROLLA, *Il difficile equilibrio tra diritti di informazione e tutela della dignità e della vita privata: brevi considerazioni alla luce dell'esperienza italiana*, consultabile su www.unisi.it/ricerca/dip/dir_eco/COMPARATO/rolla4.doc.

[7] V. RICCIUTO, *Le Finalità del Codice*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Il codice dei Trattamento dei dati personali, Giappichelli, Torino, 2007e S. RODOTà, *Tra i diritti fondamentali ed elasticità della normativa: il nuovo codice della privacy*, Eur. dir. priv., 2004, 2.

[8] S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006.

delle problematiche inerenti alla privacy e al trattamento dei dati personali, questioni che necessariamente superano i confini nazionali anche in termini di tutele e discipline.[9]

Tale aspetto rappresenta una proiezione del più ampio discorso che vede oggi la tutela dei diritti fondamentali radicata non soltanto nella prospettiva nazionale, ma nel contesto europeo ed internazionale[10].

Proprio sul rapporto fra privacy e nuove tecnologie nella società globale si concentrerà la presente trattazione, con cui, senza alcuna pretesa di esaustività, si cercherà di dare uno sguardo d'insieme: sullo sviluppo che il concetto stesso di privacy è venuto assumendo, su alcuni specifici settori, nei quali la necessità di coordinamento con il progresso tecnologico si pone maggiormente in evidenza, nonché su alcune questioni legate alla figura posta dal legislatore comunitario e nazionale a garanzia della tutela di dati personali – il Garante per la protezione dei dati personali - rispetto all'assetto istituzionale complessivo.

In particolare, la necessità di soffermarsi su alcuni settori particolari nasce dalla constatazione che solo passando dal discorso generale alle diverse applicazioni, che le singole tecnologie possono avere, ci si rende conto della diversità con cui queste devono essere trattate.

In tal modo, si potranno realizzare differenti bilanciamenti concreti di interessi e diritti che possono portare anche a risultati difformi, pur coinvolgendo la stessa tecnologia. Si parla, così, di "relativizzazione della tecnologia"[11]: La questione diventa il rapporto fra la specifica applicazione tecnologica e la tutela dei diritti che questa può andare ad incidere.

E' ormai all'evidenza di tutti come la tecnologia acquisti sempre più un forte potere di organizzazione sociale e la tesi della sua neutralità, pur importante per evidenziare la responsabilità di chi la adopera, rischia di sottovalutare che il concreto ruolo di una tecnologia deriva soprattutto

[9] U. PAGALLO, *La tutela della Privacy negli Stati Uniti D'America e in Europa*, Giuffrè, Milano, 2008, pag 31; C. DE GIACOMO, *Diritto, libertà e Privacy nel mondo della comunicazione globale*, op. cit., pag 5.; S. NIGER, *Privacy e tutela globale*, consultabile su http://www.diritto.it/materiali/informatica/niger2.html. Per una panoramica degli atti normativi e dei documenti europei si veda http://www.privacy.it/normativeu.html.

[10] G.M. FLICK, *Prefazione*, in G. SANTANIELLO (a cura di), La protezione dei dati personali , Cedam, Padova, 2005.

[11] S. RODOTà, *Laicizzare il rapporto fra innovazione e società*, in Innovazioni tecnologiche e privacy, consultabile su www.garanteprivacy.it.

dalle sue specifiche modalità d'uso. Vi sono effetti, invero, che si producono per il solo fatto di scegliere di utilizzare una determinata tecnologia[12].

Tuttavia, se l'aspetto tecnico è una prerogativa degli specialisti, le possibili conseguenze del loro utilizzo riguardano altresì la società e le sue regole: la politica, i giuristi[13] ed i giudici, nazionali e non. Ciò nonostante, è solo da una corretta sinergia fra i due aspetti che si otterranno i risultati migliori.

[12] Così S.RODOTà, *Tecnopolitica, la democrazia e le nuove tecnologie della comunicazione*, op. cit., pag. 28.

[13] S. RODOTà, *Intervista su privacy e libertà*, op cit., pag 137.

CAPITOLO PRIMO

La nascita e lo sviluppo del diritto alla privacy

SOMMARIO: 1. Origini e sviluppi storico giuridici. – 2. Lo sviluppo del diritto alla privacy negli Stati Uniti. – 3. Origine nazionale del diritto alla privacy. - 3.1 Principali fonti legislative nazionali. – 4. Il percorso europeo. – 5. Riferimenti di diritto comparato in Europa. - 5.1. La Spagna - 5.2. La Francia - 5.3. La Gran Bretagna - 5.4. La Germania.

1. Origini e sviluppi storico giuridici

I concetti giuridici di riservatezza e di privacy sono relativamente recenti. Infatti, è con l'articolo "The Right To Privacy" [14] di Warren e Brandeis che nel 1890 la nozione di privacy ha iniziato ad avere una consistenza giuridica nel *right to be let alone*, ovvero come diritto ad esser lasciato solo.

Il concetto di privacy è da principio legato al concetto di proprietà privata e ai mezzi di tutela di tale diritto.

Così concepita la privacy è lo strumento volto a tutelare una duplice esigenza:

a) la protezione della sfera privata dall'altrui curiosità;

b) il "controllo" delle informazioni in uscita dalla sfera privata verso l'esterno.

Si è fatto ricorso, cioè, alla classica definizione della proprietà come *ius excludendi alios.* La borghesia si è appropriata del suo spazio interiore secondo le stesse tecniche che gli avevano permesso di impossessarsi dello spazio fisico[15].

Com'è stato sottolineato[16], il divieto di ingresso nello spazio altrui ha rappresentato per l'appunto lo "snodo culturale" legato alla vicenda del concetto originario di privacy[17].

---

[14] S. WARREN, L. D. BRANDEIS, *The right of privacy*, in Harv.L. Rev., 1890, 4, 193.

[15] Si veda ad esempio il fenomeno delle *enclosures* in Inghilterra dalla fine del seicento.

[16] S. RODOTà, *Intervista su privacy e libertà,* op. ci.t

Ben presto, però, sono emersi l'esatta dimensione sociale del concetto e la sua rilevanza in merito alla tutela del persona come singolo e come cittadino; così nel 1971 Arthur Miller ha definito la privacy come "the individual's ability to control the circolation of information relating to him – a power that often in essential to manteining social relationship and personal freedom"[18].

Il diritto ad essere "lasciato in pace" è diventato, così, la premessa necessaria perché si possano fare liberamente una serie di scelte, garantendo il diritto di essere "pienamente esponibile", senza che questo possa essere fonte di discriminazione. Il diritto alla privacy si lega allora a quello della libertà individuale e collettiva[19] .

Con lo sviluppo odierno delle tecnologie ed il ricorso, sempre maggiore, all'utilizzo dei trattamenti dei dati personali, soprattutto automatizzati, nonché alla possibilità di scambio e aggregazione degli stessi, attraverso internet e la creazione di banche dati, le esigenze connesse alla privacy si evolvono ancora più significativamente[20].

L'uomo è ormai inserito in una società "globale", nella quale la stragrande maggioranza delle azioni compiute e delle scelte individuali lascia "tracce"; l'organizzazione di queste consente la ricostruzione di veri e propri identikit della persona.

In internet è nata un'espressione, diventata d'uso comune, di "corpo elettronico" e sono ormai all'ordine del giorno notizie riguardanti la nascita di siti, come Spock.com[21], per trovare persone celebri, ma soprattutto persone comuni. L'idea di base nasce dalle statistiche, secondo le quali il 30% delle ricerche in rete riguarda le persone. La novità di Spock.com e dei suoi successori è di mettere insieme informazioni raccolte, completarle con foto e parole chiave e collegare ciascun profilo a quello di altre persone. Attualmente sono state recensite circa 100 milioni di persone, ma l'obiettivo dichiarato è di trovare tutti gli abitanti della terra!

[17] L'autore insiste spesso sulla matrice culturale della privacy, in termini di vera e propria "cultura della privacy"; cfr anche G. DAL SASSO, *Rispetto della dignità della persona e tutela della privacy, particolarmente in sanità*, consultabile su www.formazione.eu.com/_documents/casagrande/articoli/2004-03-08articolo.pdf .

[18] A. MILLER, *The assault of privacy*, an Arbor University of Michigan Press 1971.

[19] S. RODOTà, *Intervista su privacy e libertà*, op. cit; S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, op. cit..

[20] G. TIBERI, *Riservatezza e protezione dei dati personali*, in M. CARTABIA (a cura di), I diritti in azione, Universalità e pluralismo dei diritti fondamentali nelle Corti europee, Il Mulino, 2007, pag 351.

[21] P. COPPOLA, in La Repubblica, 11 agosto 2007.

Funzione simile hanno anche il famoso e discusso Facebook e gli altri cd. social network.

Le informazioni acquisite, quindi, non sono più solamente quelle provenienti dal domicilio, più o meno ideale, bensì quelle fornite inconsapevolmente attraverso i propri dati personali "seminati" nell'ambiente.

A quest'argomento si lega, poi, anche la questione del cd. "diritto all'oblio", in forza del quale e a tutela del diritto fondamentale al libero sviluppo della propria personalità "nessuno deve essere obbligato a rimanere, senza scampo,'prigioniero del proprio passato', cosicché la diffusione di qualsiasi fatto del passato diventa legittima solo se quell'informazione è davvero essenziale"[22].

E' bene tener presente, inoltre, tutte le problematiche scaturenti dal passaggio da forme di sorveglianza mirate a forme di sorveglianza generalizzate, come quelle introdotte, dopo l'11 settembre, negli Stati Uniti con il *Patriot Act*[23].

Ancora, si guardi al caso *Echelon*[24], ovvero la rete di controllo organizzata dai cinque paesi anglosassoni (USA, Gran Bretagna, Canada, Australia, Nuova Zelanda), la cui esistenza è stata negata per molto tempo, e che in realtà ha la possibilità di controllare ogni comunicazione elettronica: telefono, fax, posta elettronica, internet.

La vicenda è uscita allo scoperto perché i francesi si sono accorti che in una serie di appalti internazionali, i concorrenti americani vincevano sempre. Le informazioni raccolte formalmente per ragioni di sicurezza, venivano in realtà trasmesse alle aziende americane[25].

Si comincia, quindi, a parlare di privacy, intendendo con tale espressione non soltanto gli aspetti tradizionali - di cui si coglie un'evoluzione nel cd. diritto ad essere lasciati in pace - inteso come esigenza di protezione del singolo dai tentativi di contatto realizzati da terzi secondo particolari

---

[22] S. RODOTà, *Intervista su privacy e libertà*, op. cit, pag. 66 e sgg.

[23] http://www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php;http://www.peacereporter.net/dettaglio_articolo.php?idpa=&idc=36&ida=&idt=&idart=4918.

[24] http://www.cli.di.unipi.it/~guidi/echelon/tesi.html.

[25] S. RODOTà, *Intervista su privacy e libertà*, Op. cit..; riguardo alla frequenza con cui in America vengono trasmessi dati inizialmente raccolti per finalità commerciali a istituzioni pubbliche con finalità di sicurezza e lotta al terrorismo, si veda il caso Matrix in U. PAGALLO, *La tutela della Privacy negli Stati Uniti D'America e in Europa.* op. cit., pag.102

modalità[26] - ma anche il potere di controllo sulla circolazione delle proprie informazioni personali[27].

Nel linguaggio internazionale l'espressione più usata è ormai quella di *data protection* e nella Carta dei diritti fondamentali dell'Unione Europea il rispetto della vita privata e la protezione dei dai personali sono distinti anche da un punto di vista sistematico, l'uno previsto dall'art 7, l'altro dall'art. 8.

Il diritto alla riservatezza-privacy viene così sempre più spesso qualificato come diritto di decidere liberamente sulla propria vita privata, come autodeterminazione informativa[28] e, indirettamente, soprattutto negli ultimi anni, ha rafforzato la coscienza di un vero e proprio "diritto all'autodeterminazione", quale diritto alla libera costruzione della propria personalità, e la conseguente esigenza di compiere liberamente scelte coerenti con i propri principi (si veda specialmente in ambito sanitario).

Lo sviluppo di massa delle tecnologie, la particolare invasività di alcune di queste e la crescente possibilità della loro reciproca interazione, con il conseguente scambio delle informazioni/dati raccolti, moltiplicano oggi esponenzialmente i rischi di violazione del diritto alla privacy.

Esempi di innovazioni tecnologiche, come visto, sono anzitutto quelle che riguardano le elaborazioni delle informazioni, le reti di comunicazione, le memorie elettroniche, i sistemi di rilevamento dei dati, del loro uso diretto ed in combinazione con la produzione industriale, la distribuzione commerciale, i trasporti ecc.

Le informazioni così raccolte vengono poi immagazzinate in banche-dati delle reti che gestiscono la sicurezza, la sanità, la ricerca, l'istruzione ecc[29].

Siamo circondati dalla tecnologia pubblica e privata, spesso, senza neanche rendercene conto. Si pensi che dal 1998 è assegnato in tutto il

[26] Es. in tema di propaganda elettorale C. Cost. 138/85 o si vedano i provvedimenti del Garante della privacy del 30 maggio 2007 nonché il relativo comunicato stampa del 15 giugno 2007 riguardo le telefonate indesiderate effettuate dai call center dei principali gestori telefonici.

[27] S.RODOTà, *Tecnologia e diritti*, op.cit; G. TIBERI, *Riservatezza e protezione dei dati personali*, in M. CARTABIA (a cura di), I diritti in azione, Universalità e pluralismo dei diritti fondamentali nelle Corti europee, op. cit., pag 351; S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*,op. cit.

[28] Cfr la famosa sentenza della Corte costituzionale tedesca del 15 dicembre 1983, la quale afferma un diritto all'autodeterminazione informativa di rango costituzionale.

[29] G. RASI, *Progresso tecnologico e sviluppo civile*, in Innovazioni tecnologiche e privacy, consultabile su www.garanteprivacy.it.

mondo il *Big Brother Award*, attribuito a coloro, soggetti pubblici o privati, che durante l'anno si sono distinti per avere realizzato progetti in qualche modo più lesivi del diritto alla privacy[30].

E' perciò necessario confrontarci con questa realtà, in modo da trovare equilibri che consentano alla tecnologia di svilupparsi nel rispetto dei diritti fondamentali della persona.

Questo, tuttavia, deve avvenire nella consapevolezza che il raccordo fra innovazione tecnologica e protezione dei dati personali, se non si presenta impossibile, è però sicuramente complesso, in quanto mosso da due forti dinamiche. Si assiste, infatti, da un lato allo sviluppo incessante delle tecnologie, caratterizzato dalla globalità dello scenario applicativo, e dall'altra alla trasformazione della riservatezza, che "da guscio protettivo della persona va evolvendo a patrimonio informativo circolante, come denominatore comune di tutte le realtà industriali, commerciali, culturali, pubbliche e private e come riferimento costante in tutti i campi di attività."[31]

2. Lo sviluppo del diritto alla privacy negli Stati Uniti

La storia statunitense del diritto alla privacy viene fatta risalire al già citato articolo di Warren e Brandeis del 1890, che l'ha definito come il *right to be let alone*[32].

La rivoluzione industriale, l'urbanizzazione di massa e la diffusione dei mezzi di informazione sono stati il contesto storico, economico e sociale in cui la borghesia ha sentito la necessità di tutelare il proprio spazio vitale da intrusioni esterne[33].

La riflessione di Warren e Brandeis è partita dalla constatazione del potente sviluppo dei mass-media e del crescente sviluppo della stampa

[30] La decima edizione si è tenuta il 29 maggio 2010 in Francia, cfr http://www.bigbrotherawards.org , mentre l'edizione italiana si è svolta il 29 maggio a Firenze, vedi http://bba.winstonsmith.info/

[31] G. SANTANIELLO, *Tipologia delle innovazioni tecnologiche e protezione dei dati personali*, in Innovazione tecnologiche e privacy, consultabile su www.garanteprivacy.it.

[32] Tuttavia, il termine *to be let alone* è stato usato per la prima volta dal giudice T. M. COOLEY, *Treatise on the law of Torts or the Wrongs Which Arise Independently of Contract*, del 1878, pubblicato da Callaghan & Company, 1907, consultabile su http://www.archive.org/details/cu31924019311426; alcuni hanno poi ritenuto che il termine privacy sia da rinvenire nel 1849 nel caso inglese Prince Albert v. Strange, tra l'altro, più volte citato nell'articolo di Warren e Brandeis.

[33] Al 1884 risale l'invenzione della prima macchina fotografica di piccole dimensioni in grado di scattare fotografie istantanee.

scandalistica, *yellow journalism*, che commercializzava gli aspetti più intimi della vita privata, quegli aspetti che un tempo non fuoriuscivano dall'ambito ristretto di cerchie di amici e conoscenti[34].

Il diritto ad essere lasciati soli è stato configurato, così, come un diritto della persona ad escludere qualsiasi ingerenza estranea all'interno delle mura domestiche, un diritto, dunque a contenuto negativo (*seclusion*).

La tesi proposta dai due giuristi americani non è stata, però, accolta subito dalla giurisprudenza statunitense. In tal senso è esemplificativa la sentenza della Corte di Appello di New York del 1902, Roberson v. Rochester Foldin Box Co., in cui è stata rigettata la richiesta di tutela del diritto alla privacy poiché "there is no precedent for such an action to be found in the decision of this court"[35].

Di conseguenza, nel 1903 sono stati emanati dallo stato di New York, seguito poi da numerosi altri stati[36], due statuti che conferivano una specifica *cause of action* all'interesse alla privacy.

Nel 1905 però la Corte Suprema della Georgia, in un caso molto simile a quello Roberson, ha rovesciato completamente la citata decisione della Corte d'Appello di New York, riconoscendo esplicitamente l'esistenza nella

[34] Così A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*. Bulzoni, Roma, 1974, pag 48: "Il merito <<storico>> di Warren e Brandeis non sta certo nella, peraltro fragile, definizione del diritto alla privacy, ma risiede piuttosto nella autonoma configurazione della violazione della <<vita privata>> come tort, ossia come illecito civile. Per loro, infatti, l'interferenza nella privacy produce un danno, identificabile nel turbamento della <<pace dello spirito>> propria del soggetto della correlativa sfera privata, che avendo tutte le caratteristiche del *dannum iniuria datum*, autorizza all'azione di inibizione o di risarcimento. Questa, e non altra, è la loro <<scoperta>>, e perciò in relazione a ad essa vanno giudicate la rilevanza e la incidenza pratica del loro contributo." Da questo punto di vista l'autore non concorda con chi ritiene che i due autori sostenessero un legame fra privacy e proprietà, anzi afferma che i due giuristi si siano scagliati esattamente contro l'impostazione dominante dell'epoca, da cui però non riescono a svincolarsi completamente: "figli legittimi del loro tempo, non percepiscono affatto le dimensioni costituzionalistiche del problema. (…) Ciò si spiega storicamente con il rilievo che il diritto privato era di fatto la struttura portante della vita giuridica, poiché nello <<Stato liberale>> ottocentesco i rapporti proprietari costituivano, non soltanto l'intelaiatura delle relazioni interprivate , ma anche la principale forma di aggregazione politica operante al di là o in mancanza dei partiti politici. Riguardo a Warren e Brendeis il più che si può dire relativamente a questi problemi è che essi sembrano percepire confusamente che l'ideologia <<liberale>> classica non è più adeguata alla società di massa e che è necessario quindi una rifondazione teorica in chiave umanitaria dei diritti di libertà. Essi, tuttavia, non riescono a superare sostanzialmente quella ideologia e perciò non riescono a scorgere i limiti del metodo giuridico che la accompagna. (…) Essi, cioè, sono totalmente immersi nel *private law of torts*, non riescono a vedere al di là dell'aspetto negativo del problema, poiché nella prospettiva che si sono scelti la privacy costituisce un problema soltanto allorché è violata (…)."op cit., pag. 64 e ss..

[35] 171 N. Y. 538, 543, 64 N.E. 442, 443 (1902).

[36] Nel 1903 dallo stato della Pennsylvania, nel 1904 da quello della Virginia, nel 1909 dalla Utah, nel 1955 dall'Oklahoma.

common law di un diritto alla privacy e definendo il suddetto interesse "derivante dal diritto naturale"[37].

A partire da questa sentenza la privacy è stata sempre più spesso riconosciuta dai giudici americani come un interesse meritevole di tutela ed il risultato di questo filone giurisprudenziale è stato consolidato[38], in un certo senso, dall'*American Law Institute* nel *Restatement of Torts* del 1939[39].

Tuttavia, è stato intuito molto presto come la formula *right to be let alone* non fosse in grado di ricomprendere tutte le ipotesi, in cui una persona ha un interesse al riserbo degno di protezione giuridica.

Dall'inizio del XX secolo sono aumentati significativamente gli strumenti di informazione di massa[40], attraverso cui si raccolgono e divulgano informazioni di ogni possibile cittadino così come sono incrementati gli archivi governativi: nel 1935 viene creato il *Social Security System* che già nel 1945 vantava la schedatura di più di 100 milioni di persone.

Sempre in quel periodo anche le imprese private hanno cominciato a creare banche dati per ragioni di marketing[41].

L'interesse alla privacy è diventato, così, un interesse dell'intera collettività, non più solo del singolo individuo.

Quanto alla giurisprudenza intervenuta fra il 1890 e il 1960, questa ha evidenziato come, in via generale, la privacy è stata invocata per la tutela di quattro principali interessi[42].

Così, alcune controversie hanno riguardato l'interesse ad impedire intromissioni di estranei nella propria sfera privata[43]. In altre si è visto

---

[37] Caso Paveish v. New England Life Insurance Company 122 Ga. 190, 194, 50 S.E. (1905). L'attore lamentava che una sua fotografica era stata utilizzata per fini pubblicitari da una compagnia assicuratrice senza il suo consenso. Cfr A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, op. cit., pag 53 e ss.

[38] Così U. M. Ubertazzi, *Diritto alla privacy, natura e funzioni giuridiche*, op. cit.

[39] Nella giurisprudenza americana , i *Restatements of the Law* sono una serie di trattati di materie giuridiche che cercano di informare i giudici e gli avvocati sui principi generali di common law. Fino ad oggi, Ci sono stati tre serie di Restatements, tutte pubblicate dall'American Law Institute , un organismo di docenti universitari e professionisti del diritto fondato nel 1923 che si occupa della riforma del diritto statunitense, vedi il relativo sito www.ali.org.

[40] Nel 1844 il telegrafo, nel 1876 il telefono. Allo stesso tempo aumentano anche gli strumenti per intercettare le conversazioni, le cd. bug (microspiee) le parabolic microphone, le wiretap, tanto che nel 1934 il Congresso emana il Federal Communication Act.

[41] Ad esempio, dal 1920 la General Motors inizia a registrare i propri clienti. Cfr T. M. UBERTAZZI, in Diritto alla privacy, natura e funzioni giuridiche, op cit.

[42] Così T.M. UBERTAZZI, *Diritto alla privacy, natura e funzioni giuridiche*, op. cit.

[43] Ad esempio, Welsh, Respondent v. Rohemet Al, 125 Mont. 517, 241, P.2d 816 (1952), l 'attore (affittuario) lamentava che il conduttore aveva occupato senza il suo consenso la sua abitazione, violando il proprio diritto alla privacy. La Corte Suprema del Montana aderendo la principio secondo cui "the house of every one is to him as his castle" ha accolto la richiesta e condannato il conduttore al

l'interesse ad opporsi alla divulgazione al pubblico di fatti privati, quali le condizioni economiche, la salute o fatti passati per cui viene invocato l'interesse all'oblio[44]. Altri giudizi, invece, sono stati inerenti all'interesse ad impedire la rappresentazione dell'individuo in modo non corretto[45]. Infine, ulteriori casi hanno avuto ad oggetto l'interesse ad opporsi all'utilizzazione di dati o allo sfruttamento della propria notorietà a profitto altrui[46].

Da questo rapido scorcio emerge come la giurisprudenza abbia progressivamente dato alla privacy un'estensione sempre maggiore, facendovi ricomprendere interessi anche molto eterogenei, come se questa fosse una "nozione ombrello" [47].

Sulla base delle indicate quattro linee di sviluppo della giurisprudenza nel 1960, Prosser ha proposto successivamente una quadri partizione dei *torts* (illeciti) relativi al diritto alla privacy: *inclusion upon seclusion*, *public disclusure of private facts*, *false light in public eye* e *appropriation*[48]. Tale quadri partizione è stata poi recepita integralmente nel 1977 dal secondo *Restatement of torts*[49].

In merito, però, altra dottrina, tra cui Bloustien, ha obiettato che il diritto alla privacy debba invero essere inteso come un diritto unitario, in quanto gli interessi sottostanti hanno tutti come minimo comune denominatore l'*human dignity*[50].

Blounstein, in particolare, si è ispirato espressamente alle posizioni del giudice Brandeis[51] e a quelle dei molti che, dopo di lui, hanno individuato il

risarcimento dei danni. Il diritto alla riservatezza è stato invocato anche fuori dal proprio domicilio, come in ospedale, sul luogo di lavoro, in una stanza d'albergo.

44 Vedi i casi Trammel v. Citizien News Company, Inc, 285 Ky. 529, 529, 148 S.W. 2d 708 (1941); Cason v. Bakin, 155 Fla. 198, 20, So.2d 243 (1945); Melvin v. Reid,112 Call. App. 285, 297 P.91 (1931).

45 Vedi ad esempio il caso Peay v. Courtis Puplishing Company, 78 F. Supp.. 305 (1948), in cui un taxista lamentava che il convenuto aveva utilizzato una sua immagine senza il suo consenso per un articolo ironico riguardo i tassisti di Washington D.C..

46 Ad es. il caso Fairfield v. American Photocopy Equipment Company, 138 Cal. App.2d 82, 86, 291, P2d 194, 197 (1954), in cui l'acquirente di una fotocopiatrice si lamentava per l'utilizzo dei propri dati, senza il suo consenso, fatto dalla società venditrice a scopi pubblicitari.

47 G. TIBERI, *Riservatezza e protezione dei dati personali*, op cit..

48 W. PROSSER, *Privacy*, in Cal. L. Rev., 1960, 48, 383.

49 Per un ridimensionamento della rilevanza nella giurisprudenza statunitense della teoria di Posser v. M. SURACE, *Evoluzione storico-giuridica del diritto alla riservatezza: da diritto borghese a sinonimo di libertà*, Analisi socio-giuridica del rapporto tra sorveglianza e diritto alla riservatezza nell'era di Internet, cap 2, consultabile su http://www.altrodiritto.unifi.it/ricerche/control/surace/cap2.htm.

50 E. J. BLOUSTEIN, *Privacy as an aspect of human dignity: an answer to Dean Prosser*, in N.Y.U. L. Rev., 1964.

51 "Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions" Giudice Louis D. Brandeis, *dissenting opinion* in Olmstead vs. U.S., consultabile su http://supreme.justia.com/us/277/438/case.html

principio generale sottostante alla nozione di privacy in quello di una personalità inviolabile. Questi autori hanno ritenuto, così, che la privacy fosse un concetto essenziale per quella ricerca della felicità, che rappresenta uno dei valori fondamentali del sistema costituzionale statunitense[52].

Un altro passo decisivo verso la formulazione di una teoria costituzionale del diritto alla privacy è stato compiuto in seguito dal giudice Douglas, in due opinioni dissenzienti[53].

In esse Douglas ha inteso la Costituzione, soprattutto nelle sue norme fondamentali, come un insieme di valori che si impongono in ogni rapporto sociale, sia a livello federale che statale. Pertanto, nell'interpretazione delle norme costituzionali sui diritti di libertà, secondo Douglas, è necessario seguire un metodo rigorosamente realistico, attento alle conseguenze politiche e sociali, giungendo, in tal modo a concepire il diritto alla privacy come "il più penetrante e comprensivo sviluppo della libertà individuale nelle Costituzioni moderne"[54].

Il concetto di vita privata, perciò, non allude ad un una generica libertà della persona, ma si riferisce al principio di ogni libertà, cosicché la privacy

[52]Ancora Brendeis: "The protection guaranteed by the Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone -- the most comprehensive of rights, and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence ", [*La protezione garantita dagli Emendamenti è molto più vasta nelle sue mire. Gli estensori della nostra Costituzione si prodigarono per assicurarci le condizioni favorevoli alla ricerca della felicità. Essi riconobbero il significato della natura spirituale di un uomo, dei suoi sentimenti, e del suo intelletto. Essi sapevano che solo una parte dei dolori, piaceri e soddisfazioni della vita si possono trovare nelle cose materiali. Hanno cercato di proteggere gli Americani nelle loro credenze, pensieri, emozioni e sensazioni. Essi hanno conferito, contro il Governo, il diritto ad essere lasciati soli - il più comprensivo dei diritti, ed il diritto più stimato dall'uomo civilizzato. Per proteggere questo diritto, ogni intrusione ingiustificabile da parte del Governo nella privacy di un individuo, qualunque sia lo strumento impiegato, deve essere considerato una violazione del Quarto Emendamento*]. Vedi M. SURACE, *Evoluzione storico-giuridica del diritto alla riservatezza: da diritto borghese a sinonimo di libertà*, op cit.

[53] Douglas, Dissentig opinion in Irvine v California, 347 U.S. 128, 149, 150 s, consultabile su http://supreme.justia.com/us/347/128/case.html#149, e in Public Utilities v. Pollak, 343 U.S. 467 s, consultabile su http://openjurist.org/343/us/451/public-utilities-commission-of-district-of-columbia-v-pollak-pollak, "Liberty in the constitutional sense must mean more than freedom from unlawful governmental restraint; it must include privacy as well, if it is to be a repository of freedom. The right to be let alone is indeed the beginning of all freedom (…)" Ancora, si legge, per la privacy, intesa come diritto all'autodeterminazione: "The right of privacy should include the right to pick and choose from competing entertainments, competing propaganda, competing political philosophies. If people are let alone in those choices, the right of privacy will pay dividends in character and integrity. The strength of our system is in the dignity, the resourcefulness, and the independence of our people. Our confidence is in their ability as individuals to make the wisest choice. That system cannot flourish if regimentation takes hold. The right of privacy, today violated, is a powerful deterrent to any one who would control men's minds."

[54] A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, op. cit., pag 152. .

viene tutelata non da una sola disposizione costituzionale, ma piuttosto dalla serie di disposizioni che riguardano le libertà fondamentali del cittadino.

Da parte sua, anche la Corte Suprema ha affrontato spesso l'argomento della fondamento costituzionale del diritto alla privacy e l'ha cercato, innanzitutto, nel quarto emendamento, in base al quale ogni individuo ha il diritto alla sicurezza della persona, del domicilio e dei beni personali a fronte di perquisizioni e sequestri irragionevoli.

Qui e nello specifico in materia di intercettazioni telefoniche compiute dai pubblici poteri, nel famoso caso Olmstead v. United Stated, inizialmente la Corte ha invero adottato una concezione domestica della privacy[55], rigettando la richiesta di tutela, poiché non vi era stato nessun *physical trespass*[56].

[55] Negli anni 60-70 questa ha caratterizzato un filone giurisprudenziale della Suprema Corte definito della "privacy in the bedroom". Si tratta di interventi su una varietà di questioni concernenti stili di vita e libertà sessuali, la cui leicità veniva riconosciuta in ragione della non passibilità del confine giuridico rappresentato dalla soglia della camera da letto, indipendentemente dal giudizio di valore ad essi relativo. V C. DE GIACOMO, *Diritto, libertà e Privacy nel mondo della comunicazione globale* op cit., 20.

[56] 277 U.S. 438, 464, 48 S.Ct 564, 568 (1924), consultabile su http://supreme.justia.com/us/277/438/case.html. Motivazione criticata da Braindeis nella sua famosa *dissentig opinion*, in cui suggeriva una lettura della Costituzione americana in grado di tenere conto dello sviluppo di nuovi strumenti tecnologici: "To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence " [*Per proteggere questo diritto, ogni intrusione ingiustificabile da parte del Governo nella privacy di un individuo, qualunque sia lo strumento impiegato, deve essere considerato una violazione del Quarto Emendamento*].

Vedi anche C. DE GIACOMO, *Diritto, libertà e Privacy nel mondo della comunicazione globale* op. cit. pag 67. A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, op. cit., pag 98 : "Citando una delle prime decisioni della Corte Suprema, manifestata per il tramite del Chief Justice Marshall, Brandeis afferma che ogni discorso sulla Costituzione deve partire dal riconoscimento della <<specialità>> della interpretazione costituzionale. In misura largamente maggiore ad ogni altro tipo di legge, la Costituzione, infatti, deve fare i conti con il suo oggetto, e cioè con la forma che storicamente assumono i rapporti sociali e con il progresso tecnico che di tempo in tempo si manifesta in una comunità. Una Carta costituzionale, perciò, non può essere interpretata in modo puramente letterale, né con il semplice ausilio delle tecniche semasiologiche, e non può essere esclusivamente vincolata ad un'errmeneusi rapportata al tempo dei costituenti o delle espressioni da questi manifestate nel corso dei lavori preparatori. Se si seguisse questa via, sostiene Brandeis, non solo non si potrebbe confrontare con al Costituzione tutta la legislazione deliberata su oggetti che in nostri Padri forse non hanno neppure pensato, ma non si terrebbe conto anche del fato che, attraverso clausole generali, come quella del Due process, viene oggi immesso nel nostro ordinamento ciò che un secolo o un secolo e mezzo fa era rigettato perché ritenuto oppressivo e arbitrario .". La frase di Marshall riportata da Brandeis è: "We must never forget that it is a constitution we are expounding", cfr. McCulloch v. Mariland 4 Wheat 316, 407 (1819).

In tema di intercettazioni, il Congresso, nel 1934, ha deciso di introdurre uno schema per regolare la sorveglianza elettronica ed ha approvato il testo del Federal Communication Act. La sezione 605 della legge proibiva a chiunque di intercettare le conversazioni protette dalla legge, e di divulgare il loro contenuto senza l'autorizzazione del mittente. Il Communication Act non riuscì ad impedire praticamente nessun tipo di intercettazione in quanto aveva creato un'apparenza legislativa facilmente aggirabile, lasciando così un vuoto normativo che avrebbe ancora tardato molti anni a colmarsi. Vedi M. SURACE, *Evoluzione storico-giuridica del diritto alla riservatezza: da diritto borghese a sinonimo di libertà,* op cit..

In seguito, nel caso Katz v. United States, invece, la Corte ha ritenuto che il quarto emendamento proteggesse persone e non luoghi e, quindi, ha dichiarato che la privacy può essere violata anche in aree accessibili al pubblico[57].

Rilevante in questa sentenza è anche la *concurring opinion* del giudice Harlan, il quale ha proposto l'utilizzo di un test, finalizzato a rendere individuabile ciò che si intende per "privato" alla luce del Quarto Emendamento. Nella successiva giurisprudenza, infatti, questo test è diventato il parametro per stabilire quando l'azione governativa violava la norma costituzionale.

In particolare, il giudice Harlan ha osservato che, nel chiedersi che tipo di protezione lo Stato dia alla privacy del singolo cittadino, la Corte dovrebbe domandarsi se: "esiste un duplice requisito, il primo dei quali è stabilire se la persona ha mostrato un'effettiva (e soggettiva) aspettativa di privacy, mentre il secondo è che quell'aspettativa sia riconosciuta dalla società come ragionevole"[58]. Soltanto nel caso in cui la Corte risponda affermativamente ad entrambe le questioni, si potrà elevare la semplice aspettativa a diritto protetto dal Quarto Emendamento[59].

La Corte ha poi rinvenuto il fondamento costituzionale del diritto alla privacy anche nel Primo emendamento, secondo il quale " il Congresso non deve emanare alcuna legge che (…) limiti la libertà di parola, o della stampa, o il diritto di riunirsi pacificamente e di agire nei confronti del governo per il risarcimento dei danni subiti".

---

[57] "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection *[…]*But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.", [*Ciò che una persona espone consapevolmente di fronte ad un pubblico, anche se si trova in casa sua o nel suo ufficio, non è sottoposto alla tutela del Quarto Emendamento. [...] Ma ciò che egli cerca di preservare come privato, anche se in un luogo accessibile al pubblico, gode di una tutela costituzionale*], 389 U.S. 347, 351, 88 S.Ct 507, 511 (1967), consultabile su http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=389&invol=347. A seguito di questa sentenza il quarto emendamento è stato spesso invocato nelle varie corti a tutela della privacy.

[58] "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable", consultabile su http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=389&invol=347

[59] Si è tuttavia osservato nella successiva giurisprudenza la "generale tendenza a contrarre la sfera della giustificabile aspettativa di privacy in conseguenza dell'evolversi tecnologico, che viene dalle corti per lo più preso come dato di fatto….la Corte Suprema non ha saputo utilizzare lo strumento offertole dal giudice Harlan nel migliore dei modi, in quanto non ha saputo valutare in maniera critica l'impatto dell'evoluzione tecnologica e delle compressioni dell'aspettativa di riservatezza che questa sempre più andava attuando", M. SURACE, *Evoluzione storico-giuridica del diritto alla riservatezza: da diritto borghese a sinonimo di libertà,* op cit..

In alcuni casi, inoltre, la Corte ha applicato il Primo emendamento per tutelare non solo l'interesse individuale, ma anche quello di un gruppo, attraverso l' *associational privacy*: esemplare in tal senso è la causa NAACP v. Alabama, in cui la Corte ha riconosciuto il diritto della National Association for the Advancement of Colored People di non ottemperare all'ordine dello Stato dell'Alabama di fornire i documenti e i dati relativi ai membri dell'associazione, in quanto legittimo esercizio del diritto alla privacy [60]. Questo tuttavia non ha impedito che in altre ipotesi, invece i giudici abbiano dato, la prevalenza al diritto d'informazione[61].

Infine, la Corte Suprema ha ulteriormente individuato il fondamento del diritto alla privacy non in singoli emendamenti, bensì nella Costituzione complessivamente considerata: si vedano al riguardo le sentenze Griswold v. Connecticut del 1965, in cui la Corte ha riconosciuto la presenza "in penombra" del diritto alla privacy in più di 10 articoli della Costituzione[62], e Whalen v. Roe del 1977, in cui la Corte ha dichiarato che la Costituzione protegge una *zone of privacy*[63].

Come precedentemente osservato, lo sviluppo delle tecnologie e dei mezzi di comunicazione ha influenzato fortemente il concetto di privacy. In tal senso, già Westin la definiva come "la pretesa degli individui, gruppi e associazioni, di determinare loro stessi quando, come ed in che misura le informazioni sul loro conto sono comunicate ad altri"[64] e, come già evidenziato, Miller osservava come "l'attributo di base per un diritto effettivo [alla privacy] è la possibilità dell'individuo di controllare la circolazione delle informazioni che lo riguardano[65].

Ancora, secondo Charles Fried la privacy "non è semplicemente l'assenza di informazioni su di noi nella mente degli altri; piuttosto è il

[60] 357 U.S. 449 (1958), consultabile su http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=357&invol=449. Tra le altre Bates v. City of Little Rock, 361 U.S. 516 (1960); Shelton v. Tucker, 364 U.S. 479 (1960).

[61] Così ad esempio in Cox Broadcasting Corp. V. Cohon 420 U.S. 469 (1975)

[62] 381 U.S. 479, 484, 85 S. Ct. 1678, 1682 (1965), consultabile su http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=381&invol=479.

[63] 429 U.S. 589 (1977), consultabile su http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=429&invo l=589. I principi espressi dalla Sentenza sono stati ripresi e consolidati da numerose altre sentenze anche di corti federali.

[64] A.F. WESTIN, *Privacy and freedom*, op. cit..

[65] A. R. MILLER, *Personal privacy in the computer age: The challenge of a new technology in an information-oriented society*, in Mich. L. Rev., 1969, 67, 1107.

controllo che noi abbiamo sulle informazioni che ci riguardano"[66], avvicinandosi così ad una prospettiva multidimensionale[67].

In seguito, anche la giurisprudenza americana ha spostato l'attenzione sulla tutela dell'aspetto dinamico della privacy, inteso questo come potere di controllo sulla circolazione dei propri dati personali. In merito è indicativa la sentenza della Corte Suprema nel caso United States Department of Justice v. Reporters Comm. For freedom of press[68].

Se dal fronte dello sviluppo giurisprudenziale e dottrinale si passa successivamente a quello normativo, si osserva che in tema di privacy la legislazione americana si caratterizza, in primo luogo, per essere un sistema eminentemente "settoriale".

Sebbene, infatti, esistano numerose leggi federali e statali, nonché una nutrita giurisprudenza, ciò che in realtà manca è un quadro normativo generale che orienti e disciplini un diritto che spesso finisce per frammentarsi nelle disposizioni degli stati federati[69] e nell'autoregolamentazione delle imprese.

A livello di legislazione federale uno degli atti legislativi più importanti è il *Privacy Act* del 1974[70]. Tale testo, nato dal crescente timore dei cittadini di essere schedati, ha attribuito alla persona un diritto di cognizione, d'accesso e di rettifica dei propri dati.

Tuttavia, pur essendo il primo testo legislativo federale volto a regolare il diritto alla privacy, è stato oggetto di numerose critiche per le carenze in esso evidenziate, a partire dalla definizione di dati personali.

Il *Privacy Act*, infatti, ha escluso numerosi dati relativi all'individuo dall'applicazione della legge. Un'altra carenza è stata rinvenuta nel fatto che la normativa ha accordato alle Agenzie pubbliche la facoltà di non sottostare al divieto di *disclosure* di informazioni, qualora queste siano usate *for a rutine use.*

---

[66] C. FRIED, *Privacy*, in Yale L. Rev, J. 1968, 77, 482.

[67] "multi-dimensional prospective on the nature of a person's interest in personal data", P. SAMUELSON, *Privacy as intellectual property?*, in Stan . L. Rev., 2000.

[68] 489 U.S. 749 763 109 S. Ct. 1468, 1476 (1989), consultabile su http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl? court=us&vol=489&invol=749.

[69] U. PAGALLO, *La tutela della Privacy negli Stati Uniti D'America e in Europa*, op. cit.

[70] Consultabile su http://www.justice.gov/opcl/privstat.htm.

Inoltre, il *Privacy Act* ha regolato la raccolta e l'utilizzo di dati solo nel settore pubblico e si applica solo alle Agenzie federali, non a quelle statali e locali.

Sono previste, inoltre, eccezioni al divieto di diffusione dei dati, nel caso in cui questi siano trasmessi al *Census Bureau* (Ufficio del censimento). Altre limitazioni sono state apportate dal *Freedom of Information Act*, che nel 1996 il Congresso ha reso esplicitamente applicabile anche alle informazioni e agli archivi elettronici, grazie all'approvazione dell' *Electronic Freedom of Information Act*[71].

A seguire il *Privacy Act*, sono stati emanati altri testi legislativi federali per regolare il diritto alla privacy in specifici settori: ad esempio, il *Family educational rights and privacy Act* del 1974[72]; il *Foreign intelligence surveillance Act* del 1978[73]; il *Right to financial privacy Act* del 1978[74]; il *Privacy protection Act* del 1980[75]; il *Cable communications policy Act* del 1984[76]; *l'Electronic communications privacy Act* del 1986[77]; il *Video privacy protection Act* del 1988[78]; l'*Employee polygraph protection Act* del 1988[79]; il *Telephone consumer protection* Act del 1991[80]; il *Driver's privacy protection Act* del 1994[81]; il *Telecommunications Act* del 1996[82]; il

[71] Consultabile su http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm ; cfr M. SURACE, *Evoluzione storico-giuridica del diritto alla riservatezza: da diritto borghese a sinonimo di libertà,* op. cit..

[72] Volto a tutelare il diritto alla riservatezza degli studenti.

[73] Emanato a seguito della decisione della Corte Suprema nel caso UNited States v. U.S. District Court, 407 U.S: 297 (1972), regola l'attività di raccolta dei dati effettuata dai servizi segreti stranieri. Il suo campo d'azione è stato recentemente ampliato dall'USA Patriot Act.

[74] E' finalizzato alla tutela degli individui in riferimento al trattamento dei dati finanziari effettuato da federal agencies. Non si applica al settore privato.

[75] Tutela la privacy dei giornalisti.

[76] Tutela il trattamento dei dati dei sottoscrittori di un contratto di "cable service".

[77]Con i successivi emendamenti (*Omnibus Crime Patrol and Safe Streets Act*), è servito ad ampliare il raggio d'azione della legge precedente, proibendo intercettazioni non autorizzate, ed anche la diffusione di una serie di comunicazioni elettroniche, incluse le email. Per comunicazioni elettroniche l'ECPA intende ogni trasferimento di segni, segnali, scritti, suoni, dati, qualunque tipo di informazione, che venga trasmessa attraverso le reti di telecomunicazione e via cavo, inclusi i cellulari e le comunicazioni attraverso reti private, che riguardino il commercio interstatale o con l'estero.

[78] Regola la raccolta e la comunicazione di informazioni relative a persone che noleggiano videocassette.

[79] Tutela la privacy dei lavoratori.

[80] Finalizzato alla tutela dell'utente di servizi telefonici.

[81] Proibisce la diffusione di dati personali contenuti i registri automobilistici.

[82] Stabilisce obblighi in capo ai "telecommunications carirers".

Children's on line privacy protection Act del 1998[83]; il *Financial services modernization Act* del 1999[84]; *Genetic Information Non- Discrimination Act* del 2008.

Oltre alla settorialità della legislazione federale, messa in evidenza, si deve osservare anche l'ampio margine di manovra e discrezionalità lasciato ai singoli stati federali e all'autoregolamentazione privata.

In materia di privacy, esistono, infatti, "almeno cinquanta normative differenti – quanti sono gli Stati dell'Unione - che s'intrecciano con ambiti così diversi dell'ordinamento come possono essere la quiete e la pace familiare, la protezione della proprietà privata e la tutela del domicilio, gli interessi economico-finanziari e i diritti di proprietà intellettuale, fino alla sfera dell'integrità fisica rispetto ai contatti indesiderati, percosse e aggressioni"[85].

A differenza della tutela costituzionale e federale della privacy, le quali, come si è visto, vertono principalmente sui rapporti fra governo e individui, la legislazione ordinaria degli stati federati riguarda soprattutto l'ambito delle relazioni tra privati cittadini e si unisce alla tutela della privacy accordata dalla common law, a titolo di responsabilità civile, che quasi tutti gli Stati riconoscono[86].

Vanno, infine, tenute presenti le numerose leggi emanate a seguito del *Patriot Act* del 2001, le quali, con la finalità dichiarata di garantire la sicurezza nazionale e la lotta contro il terrorismo, hanno in realtà condizionato pesantemente la libertà personale nonché il diritto alla privacy e, come si vedrà più avanti, non solo nei confronti dei cittadini americani[87]. Questo evidenzia ancora di più i limiti strutturali dell'approccio settoriale prevalente nell'ordinamento americano[88], ai fini di un'efficace tutela dei diritti.

---

[83] Proibisce a qualsiasi operatore di un servizio website diretto a bambini di raccogliere illegittimamente informazioni.

[84] Consente a determinate financial institutions di scambiarsi dati relativi ai consumatori, prevedendo però l'adozione da parte delle stesse di privacy policy nei confronti dei consumatori.

[85] U. PAGALLO, *La tutela della Privacy negli Stati Uniti D'America e in Europa*, op. cit., pag 86.

[86] Per approfondimenti, U. PAGALLO, *La tutela della Privacy negli Stati Uniti D'America e in Europa*, op. cit..

[87] Parla di misure liberticide, fra i tanti ad esempio U. PAGALLO, *La tutela della Privacy negli Stati Uniti D'America e in Europa*, op cit., pag 98.

[88] "la mancanza di una normativa generale rappresenta uno dei maggiori ostacoli per garantire la piena tutela della privacy negli Stati Uniti sia rispetto al settore privato sia a quello pubblico". Conclusione cui è giunto *Electronic Privacy Information Center*, nel volume a cura di EPIC, Privacy and Human Right, Washington-London 2002 pag 4.

Tale ordinamento, tra l'altro, non prevede, come in Europa, un'apposita Autorità di garanzia, ma si caratterizza in compenso per l'estremo attivismo delle associazioni a tutela della privacy, come l'*American Civil Liberties Union*[89], l'*Electronic Privacy Information Center* [90] e l'*Electronic Frontier Foundation*[91].

3. Origine nazionale del diritto alla privacy

In Italia, l'ampio dibattito dottrinale e gli orientamenti oscillanti della giurisprudenza si sono sviluppati e sono dovuti alla mancanza nell'ordinamento, prima della legge n. 675/96, di una norma espressa che riconoscesse tutela, in via generale, al diritto alla riservatezza.

Di conseguenza, il suo fondamento giuridico si è ricercato inizialmente in alcune norme del Codice civile, poi nella Carta Costituzionale e nei testi internazionali.

L'espressione diritto alla riservatezza è entrata nel linguaggio giuridico italiano per opera soprattutto del Ravà e del De Cupis. In particolare, quest'ultimo l'ha definita come "quel modo di essere della persona il quale consiste nell'esclusione dell'altrui conoscenza di quanto ha riferimento alla persona medesima"[92] e ne ha individuato il fondamento positivo nel diritto all'immagine, di cui all'art 10 del Codice civile, suggerendone l'estensione in via d'analogia ad interessi della persona accumunati da una *eadem ratio*.

Tale ricostruzione si inserisce, come noto, nel quadro complessivo operato dell'autore di una struttura pluralistica dei diritti della personalità, risultante da una molteplicità di aspetti della persona, ognuno con caratteristiche peculiari e dotato di propria autonomia.

Alla costruzione dei diritti della personalità come pluralità di diritti si è contrapposta altra dottrina, fra cui Giampiccolo[93], il quale sull'esempio della dottrina tedesca, ha preferito delineare un unico diritto della personalità, cd.

[89] www.aclu.org.

[90] http://epic.org.

[91] www.eff.org.

[92] A. DE CUPIS, *I diritti della personalità* , Vol.I, Giuffrè, Milano, 1973.

[93] G. GIAMPICCOLO, *La tutela giuridica della persona umana e il cd. diritto alla riservatezza*, in Riv. Trim. dir. Proc. Civ., 1958, pag 465-466.

teoria monista. Egli, si è mosso, infatti, dalla considerazione della persona umana come valore unitario, di conseguenza le singole norme non rappresentano il presupposto di tanti autonomi diritti della personalità, bensì la disciplina specifica di alcuni aspetti particolari della sua tutela[94].

Senza approfondire in questa sede i due filoni dottrinali, per quello che qui interessa evidenziare, quest'ultima teoria ha riportato particolari consensi anche a livello giurisprudenziale, e si è poi fondata, a livello costituzionale, sull'art. 2 ai fini di garantire l'integrale tutela della persona.

In questa prospettiva l'art. 2 Cost. non è più una formula riassuntiva dei diversi diritti della persona costituzionalmente riconosciuti, ma una clausola generale attraverso la quale operare un continuo adeguamento delle garanzie giuridiche[95].

Sempre in quegli anni, una terza linea interpretativa, pur riconoscendo l'esigenza di protezione del diritto alla riservatezza, tuttavia, ha negato alla stessa una protezione *de iure condito.*

In particolare Pugliese[96] ha contestato l'applicabilità dell'art 10 c.c. e 96-97 l. a., sostenendo da un lato che queste norme pongono limiti alla libertà di espressione e sono, quindi, norme eccezionali, dall'altro, che la tutela dell'immagine è in grado di proteggere solo le sembianze della persona, ma non la segretezza delle vicende relative alla sua vita privata.

Rilievi simili sono stati sollevati anche sull'utilizzo delle norme a tutela dell'onore, del segreto epistolare e del nome[97].

Da quanto brevemente indicato, emerge come il problema principale degli studiosi fosse proprio quello di individuare nel nostro ordinamento una normativa, da cui poter desumere una tutela generale del diritto alla privacy.

---

[94] S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali* , op. cit.

[95] "A questa stessa concezione dei diritti della personalità si uniformano le più recenti elaborazioni di nuove modalità di tutela della persona, contro aggressioni rese possibili dalla diffusione dei mezzi di comunicazione di massa e dai molteplici impieghi degli elaboratori elettronici nella raccolta , conservazione e diffusione delle informazioni" M. BESSONE, G. FERNANDO, *v. Persona fisica. a) Diritto Privato*, Enc. Dir, 1983, pag 209.

[96] G. PUGLIESE, *Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche*, nota a Trib. Roma, 14 settembre 1953, in Foro it., 1954, I, 116; vedi. T.M. UBERTAZZI, *Diritto alla privacy, natura e funzioni giuridiche*, op. cit. pag 54.

[97] Vedi F. MASCI, *Osservazioni critiche circa l'ammissibilità del diritto alla riservatezza*, in AAVV, Il diritto alla riservatezza e la sua tutela penale: Atti del terzo simposio di studi di diritto e procedura penali, Varenna, Villa Monastero, 5-7 settembre 1967/ promosso dalla Fondazione "Avv. Angelo Luzzani" di Como - Giuffrè, Milano, 1970, pp. 368 ss.

Tale fondamento è stato anche cercato nell'art. 8 della Convenzione Europea dei diritti dell'uomo e delle liberta fondamentali, nell'interpretazione estensiva fattane dalla Corte europea dei diritti dell'uomo[98], come si avrà modo di illustrare in seguito.

Quanto alla Costituzione, come già visto riguardo alle origini della privacy negli Stati Uniti, spostare l'ambito di ricerca del fondamento del diritto dal solo diritto privato all'ambito costituzionale non rappresenta solo un diverso approccio metodologico, ma una vera e propria scelta di valore.

Pertanto, come giustamente osservato, "la ricerca del fondamento costituzionale si pone come un prius logico- giuridico senza il quale qualsiasi riconoscimento sarebbe, anche esplicito, ma di livello gerarchicamente inferiore, sarebbe destinato a ritrarsi incondizionatamente davanti al contrasto con libertà aventi invece rango costituzionale, senza possibilità di effettuare eventuali bilanciamenti"[99].

Nella Carta costituzionale, infatti, pur essendo individuabili norme che difendono particolari aspetti del diritto alla riservatezza, allo stesso tempo sono espressamente riconosciute alcune libertà (es. quella di manifestare il proprio pensiero) che in caso di conflitto possono atteggiarsi a limite alla riservatezza.

Tra le norme costituzionali addotte come indici a sostegno del diritto in esame figura l'art. 13, che sancisce la libertà personale e vieta la violenza fisica e morale.

Così, secondo alcuni autori[100], attraverso la libertà morale, l'ordinamento protegge l'individuo contro "illecite interferenze nella sua sfera psichica ed in particolare riguardo al potere di autodeterminazione, interesse fondamentale della persona umana. Tale libertà di autodeterminazione, potrebbe, tuttavia, essere notevolmente compromessa dalla negazione di

[98] Alcuni hanno però ritenuto che l'art 8 fosse una norma talmente generica da poter essere solo programmatica, tra questi vedi D. ONDEI, *Due licenze esegetiche: diritto alla riservatezza e diritto di cronaca*, Milano, 1965, pag 465; R. TOMMASSINI, *Osservazioni in tema di diritto alla privacy*, in Dir. Famiglia, 1976, pag. 255. Mentre altri l'hanno considerata, invece, come norma precettiva: vedi T. A. AULETTA, *Riservatezza e tutela della personalità*, Giuffrè, Milano, 1978, pag 51, secondo il quale alle norme della Convenzione "è sempre possibile dare loro quella completezza di cui hanno bisogno facendo riferimento alle altre norme presenti nell'ordinamento.". Alcuni, ad es. M. GIORGIANNI, *La tutela della riservatezza*, in Riv, trim. dir e proc. Civ., 1970, pag. 24, hanno osservato che la Cedu regola i rapporti fra Stato e cittandino, non fra privati, pertanto, non potrebbe essere invocata in tutti quei casi la violazione del diritto alla riservatezza fosse opera di un privato a danno di un altro.

[99] M. PROSPERI, *Il diritto alla riservatezza nell'ordinamento costituzionale*, consultabile su http://www.dirittoproarte.com/dirarti/costituzione.htm.

[100] Es. M. BARBERA, *I principi costituzionali della libertà personale*, Giuffrè, Milano, 1967.

tutela alla riservatezza. Non è dubitabile, infatti, che l'individuo ha interesse a non fare conoscere certe idee o certe vicende in ambienti nei quali sarebbero causa di riprovazione e addirittura di discriminazione", inducendo l'individuo a compiere scelte non sentite, ma conformi al modo di pensare comune, pregiudicando la sua libertà di autodeterminazione e quindi li libero sviluppo della persona medesima.

"In tal modo la rilevanza costituzionale dell'interesse alla riservatezza risulta indirettamente dalla protezione che l'ordinamento assicura alla libertà morale e più specificatamente alla libertà di autodeterminazione"[101].

Alla libertà personale viene, così, ricondotto anche l'aspetto dinamico del diritto alla privacy, "ovvero il diritto di controllare nella vita di relazione, la rivelazione e l'uso pubblico di dati, notizie e informazioni che siano attinenti alla propria persona e risultino in grado di porre quest'ultima in una posizione deteriore o in una falsa luce agli occhi della gente"[102].

Altre norme costituzionali in cui è stata rinvenuta la tutela del diritto alla privacy sono l'art 14 e l'art 15, rispettivamente, a garanzia del domicilio e della libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione.

In particolare, si è affermato che la libertà di domicilio si fonda sul "diritto all'esclusività di presenza umana nella sfera privata domiciliare"[103], configurando così il domicilio come luogo privilegiato nel quale la personalità umana può svolgersi, senza interferenze esterne, tutelandolo in maniera forte da intrusioni[104]. Mentre, se si considera la privacy come aspetto della libertà e segretezza della corrispondenza, è soprattutto con le comunicazioni elettroniche che il fenomeno acquista importanza[105].

Gran parte della dottrina ha ritenuto, però, che le suddette disposizioni si riferiscono solo ad aspetti parziali della riservatezza e per questo "non offrono alcun criterio per formulare una norma generale"[106].

---

[101] T. A. AUELETTA, *Riservatezza e tutela della personalità,* op .cit., 34.

[102] A. BALDASSARE, *Diritti della persona e valori costituzionali*, Giappichelli, Torino, 1997.

[103] Idem, pag 59.

[104] Sul punto si vedano T. MARTINES , *Diritto costituzionale*, Giuffrè Milano, 1997 pag 653; A. PACE, *La video registrazioni "ambientali" tra gli artt. 14 e 15 Cost*., in Giur. Cost.,. 2002, pag 1075.

[105] Vedi M. ATELLI, *Chiamate indesiderate. Commento*, in AAVV, Privacy e telecomunicazioni. Commentario al D.lgs. n 172 /1998, Napoli, 1999.

[106] A. BELVEDERE, *Riservatezza e strumenti d'informazione*, in Dizionario del dir. priv., Milano, 1980, p. 750. Vedi tra gli altri F. MANTOVANI, *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in AAVV, Il diritto alla riservatezza e la sua tutela penale, op. cit., pag 387; F.

Pertanto, l'atteggiamento più diffuso è in generale di sfavore verso l'utilizzo delle tre norme come esclusiva base costituzionale del diritto alla riservatezza[107].

Anche l'art. 21 della Cost. è stato utilizzato dagli interpreti in relazione alla riservatezza, anche se con due finalità opposte, l'una volta a negare la rilevanza costituzionale del diritto in questione, perché ritenuto incompatibile con la liberta di espressione, l'altra, invece, a fondarne la sua rilevanza costituzionale.

La prima tesi è partita dal presupposto che l'art. 21, considerato in positivo, tutela la libertà di manifestare il proprio pensiero con qualsiasi mezzo di diffusione. Tuttavia, sebbene questa sia effettivamente una delle libertà che più spesso viene in conflitto con l'interesse alla riservatezza (vedi nell'attiva giornalistica, ad esempio), l'osservazione non sembra comunque risolutiva per escludere la rilevanza costituzionale della riservatezza, poiché i valori costituzionali vivono e si attuano attraverso il bilanciamento con altri interessi, anch'essi costituzionalmente rilevanti, che nel caso concreto vengono in rilievo[108].

Pertanto, la tutela costituzionale alla libera manifestazione del pensiero non può implicare di per sé la negazione alla riservatezza dello stesso rango costituzionale.

La seconda tesi[109] ha osservato, invece, che così come l'art 21 riconosce il diritto a manifestare il proprio pensiero, allo stesso modo prevede anche la libertà di tacere, di manifestare parzialmente il proprio pensiero o di rivelarlo soltanto ad alcuni soggetti e non altri. Pertanto, secondo questa

---

BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in AAVV, Il diritto alla riservatezza e la sua tutela penale, op. cit., pag 80.

[107] Così M. PROSPERI, *Il diritto alla riservatezza nell'ordinamento costituzionale*, op cit. Per tutti vedi A. PIZZORUSSO, *Sul diritto alla riservatezza nella Costituzione italiana*, in Prassi e Teoria, 1976, p. 37: «pur contribuendo indubbiamente alla tutela della riservatezza, le norme di questo tipo non possono dunque essere considerate come il fondamento di un corrispondente diritto costituzionale, ma soltanto essere utilizzate per operazioni interpretative dirette a combinare insieme gli effetti di precetti diversi».

[108] "(…)pressoché ogni conflitto giuridico si trova in un immaginario spazio giuridico nel quale si sovrappongono le aree di protezione di due o più diritti o interessi costituzionali", R. BIN, *Ragionevolezza e divisione dei poteri*, in «Diritto & Questioni pubbliche», 2, 2002, p. 123, consultabile su www.dirittoequestionipubbliche.org,. Sul fatto che l'individuazione di limiti impliciti ai diritti costituzionali presupponga un'operazione di bilanciamento vedi R. ROMBOLI, *Il significato essenziale della motivazione per le decisioni della Corte costituzionale in tema di diritti di libertà pronunciate a seguito di bilanciamento tra valori costituzionali contrapposti*, in V. ANGIOLINI (a cura di), Libertà e giurisprudenza costituzionale, Giappichelli, Torino, 1992, pp. 206-220. Per una sintesi della questione dei conflitto e del bilanciamento fra diritti vedi G. PINO, *conflitto e bilanciamento fra diritti individuali. Una mappa dei problemi*, consultabile su http://www.unipa.it/gpino/Conflitto%20e%20bilanciamento.pdf.

[109] A. CATAUDELLA, *La tutela civile della vita privata,* Giuffrè, Milano, 1972, pag 32.

ricostruzione tutte le attività di terzi finalizzate a conoscere e diffondere il pensiero che un individuo non vorrebbe manifestare, lederebbero la sua libertà negativa, garantita dall'art. 21[110].

Una delle norme, invece, che consente un approccio generale alla tutela della riservatezza è stata individuata nell'art 3[111] Cost., il quale garantisce il diritto alla dignità umana ed il libero sviluppo della persona umana.

La dottrina favorevole al suo utilizzo dell'art 3, come fondamento della generale tutela costituzionale del diritto alla riservatezza, ha messo in evidenza la necessità della garanzia di una sfera privata inviolabile, affinché la dignità e lo sviluppo della personalità siano effettivamente assicurati e non restino, invece, lettera morta[112].

Oltre a ciò, si è anche osservato che non solo il principio-valore della dignità è in grado di investire tutti gli aspetti della vita umana, ma nell'art. 3 Cost. la dignità "appare qualificata in senso sociale, con un ulteriore allargamento della prospettiva e una conferma della illegittimità di una lettura in chiave unicamente individualistica"[113].

Ancora, proprio perché la riservatezza riguarda un valore essenziale della persona, il relativo diritto è stato fatto rientrare fra quelli inviolabili, sanciti dall'art. 2 Cost. [114].

Inoltre, il riferimento all'art. 2 Cost. assume rilievo, dal punto di vista del riconoscimento e della garanzia dei diritti inviolabili dell'uomo, anche per il

---

[110] M. PROSPERI, *Il diritto alla riservatezza nell'ordinamento costituzionale*, op. cit.; sulla pari dignità della libertà del parlare e di tacere, vedi A. CERRI, *Libertà negativa di manifestazione del pensiero e di comunicazione - diritto alla riservatezza: fondamento e limiti*, in Giur. Cost., 1974, I, pag. 611 e ss. Contra: A. PIZZORUSSO, *Sul diritto alla riservatezza nella Costituzione italiana*, op. cit., p. 38, secondo l'autore il difetto di questa tesi sta "nel fatto che essa non tiene conto della circostanza che la tutela spettante alla libertà "negativa" di manifestazione del pensiero non può essere identica a quella propria della corrispondente libertà "positiva" giacché, mentre può ammettersi che, almeno di regola, sia rimesso all'insindacabile volontà del singolo il potere esclusivo di decidere se manifestare o meno un'opinione oppure una notizia, è invece evidente che al singolo come tale normalmente non è rimesso un corrispondente potere di tenere segreta qualunque opinione o qualunque notizia", pena l'annullamento del diritto di cronaca.

[111] S.NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, op cit., pag 47; M. PROSPERI, *Il diritto alla riservatezza nell'ordinamento costituzionale*, op cit..

[112] Contra ad es. S. FOIS, *Questioni sul fondamento costituzionale del diritto all'<<identità personale>>*, in AAVV, L'informazione e i diritti della persona, Jovene, Napoli, 1983, pag 167; F. BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, op cit., pag 84.

[113] S. RODOTà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in Rivista critica di diritto privato, 1997, pag 595.

[114] Vedi V. CRISALFULLI, L. PALADIN, *Commentario breve alla Costituzione*, Cedam, Padova, 1990; A. PIZZORUSSO, *lezioni di diritto costituzionale*, in "Il foro italiano", Roma, 1978; G ROLLA, *Le prospettive dei diritti della persona alla luce delle recenti tendenze costituzionali*, in "Quaderni costituzionali", 1997; ID, (a cura di), *Tecniche di garanzia dei diritti fondamentali*, Giappichelli, Torino, 2001.

legame che si instaura tra persona e formazioni sociali e per l'esplicita previsione di doveri inderogabili di solidarietà economica, politica e sociale.

L'art 2 Cost. esprime, poi, il principio personalista che connota l'intero testo costituzionale, individuando una priorità di valore nella persona umana.

La possibilità di fondare il rango costituzionale della riservatezza sull'art. 2 Cost. è stata discussa in vario modo. La questione principale, all'interno della quale si può a grandi linee circoscrivere il dibattito, ha riguardato la natura la funzione dell'art 2 Cost.[115].

La spaccatura dottrinale[116] verte tutt'ora invero sull'interpretazione dell'articolo come clausola generale aperta[117], tale da non considerare l'elenco dei diritti come un numero chiuso, oppure come una norma che riassume in sé i diritti positivamente previsti nel testo costituzionale[118]. Un'interpretazione in un certo senso mediana, invece, da un lato riconosce l'esigenza di conferire attraverso l'art 2 Cost. un certo grado di elasticità alla Costituzione, consentendole di adeguarsi ai mutamenti storici e sociali, dall'altra avverte della necessità di non permettere che la norma in esame diventi un varco incontrollato[119].

---

[115] Vedi T. MARTINES, *Diritto Costituzionale*, Giuffè, Milano, 2000; P. PERLINGIERI, *La personalità umana nell'ordinamento giuridico.* Camerino-Napoli, 1972; A. PIZZORUSSO, Lezioni di diritto costituzionale, in Foro It., 1984 i quali sostengono che l'importanza dell'art. 2 Cost. nel dibattito dottrinale e giurisprudenziale del diritto alla privacy discende soprattutto dall'interpretazione della norma come clausola aperta, inclusiva di diritti non riconosciuti espressamente dalla Costituzione

[116] Sul tema, vedi A. PACE, *Problematica delle libertà costituzionali*, Cedam, Padova, 2003, III edizione, pag 20ss.

[117] Es vedi A. BARBERA, *Commento all'art. 2 della Costituzio*ne , in G. BRANCA (a cura di), Commentario della Costituzione, Zanichelli, Bologna 1975 e Idem, *Nuovi diritti: attenzione ai confini*, in L. CALIFANO (a cura di), Corte costituzionale e diritti fondamentali, Giappichelli, Torino 2004, p. 19 ss; T. A. AULETTA, *Riservatezza e tutela della personalità*, op. cit., pag 42-43

[118] Es vedi A. CERRI, Regime delle *questue: violazione del principio di uguaglianza e tutela del diritto alla riservatezza*, in Giur. Cost. 1972, il quale ritiene che l'importanza discenda da una interpretazione della norma come fattispecie chiusa, cioè riferibile ai soli diritti riconosciuti in altre norme costituzionali. La tutela della riservatezza discenderebbe, quindi, dall'art. 21 come libertà di non manifestazione del pensiero.

[119] Secondo questa tesi intermedia, il diritto alla riservatezza troverebbe, in via interpretativa, il suo fondamento come principio non scritto della Costituzione. Vedi A. PIZZORUSSO, *Sul diritto alla riservatezza nella Costituzione italiana*, op. cit. pag 33 ss.; R. ROMBOLI, *La relatività dei valori costituzionali per gli atti di disposizione del proprio corpo*, in Pol. del dir., 1991, pag 565 ss.; Cfr anche la Relazione predisposta in occasione dell'incontro della delegazione della Corte costituzionale con il Tribunale costituzionale della Repubblica di Polonia, Varsavia, 30-31 marzo 2006 "la giurisprudenza della Corte non ha mai chiarito *ex professo* se tale disposizione (art 2 cost) costituisca una clausola 'chiusa', nel quale caso esse si porrebbe quale norma di principio sostanziata unicamente dal rinvio ai successivi singoli diritti nominati dalla Costituzione, ovvero debba intendersi come clausola 'aperta', tramite cui si consentirebbe l'enucleazione di 'nuovi diritti', quelli provenienti dai bisogni storicamente emergenti nel progresso e nell'evoluzione della coscienza sociale. Rimane comunque per fermo che la Corte, qualora sia chiamata in un giudizio di legittimità costituzionale ad esaminare l'ambito di applicazione di una libertà fondamentale ad una determinata fattispecie, non si può omettere di considerare se il profilo del parametro di costituzionalità evocato – esemplificando, il principio di uguaglianza (art 3) o il principio di libertà personale (art 13) – introduca un nuovo aspetto di un principio fondamentale, suscettibile o meno di autonoma

Spostando queste considerazioni alla problematica, qui esaminata, del fondamento costituzionale del diritto alla riservatezza, "si può ritenere che l'art 2 Cost. non offre un'apertura generica alla possibilità di riconoscere una tutela costituzionale diretta a tali situazioni soggettive, ma abilita ad enucleare da molteplici disposizioni costituzionali in materia di singoli profili della personalità umana che rinvengono nella Costituzione una tutela diretta e che, nel loro complesso, concorrono a delineare un riconoscimento indiretto del diritto che ogni persona ha ad avere una vita privata.

L'attività interpretativa non possiede, in questo caso, natura creativa in senso proprio, ma meramente accertativa, poiché esplicita e storicizza la portata di diritti connessi a dei valori che sono già stati positivamente codificati. Grazie all'intermediazione della clausola generale contenuta

---

considerazione e di autonoma garanzia giurisdizionale; con ciò si allude all'enucleazione di quei nuovi diritti, quali il diritto alla privacy, il diritto all'ambiente, il diritto alla tutela da manipolazioni genetiche etc, caratterizzanti la tipica società moderna, in perenne evoluzione.

Occorre, quindi, tenere presente che i diritti inviolabili, siano essi esplicitamente previsti o desunti per implicito dalla Costituzione, rappresentano una vera e propria manifestazione del 'principio personalistico': tale principio invita ad una considerazione del soggetto non quale monade isolate e avulsa dal 'mondo', bensì appunto come 'persona', tale proprio in quei rapporto sociali di relazione che soli la sostanziano. E' solo in tale modo che, d'altronde, prende corpo la realtà della moderna società pluralistica, con i suoi tipici fenomeni di interessi, bisogni, valori, che spesso sono in conflitto fra loro. Ed è proprio in quest'ambito che si inserisce uno dei più delicati compiti cui è chiamata la Corte: essa deve operare un complesso bilanciamento di valori costituzionali affinché l'esercizio di un diritto fondamentale non venga a configgere con altri interessi di vario livello", I diritti fondamentali nella giurisprudenza della Corte costituzionale, consultabile su http://www.cortecostituzionale.it/informazione/file /STU185 principi.pdf.. Vedi sull'interpretazione della costituzione in relazione ai diritti fondamentali quanto commentato da R. ROMBOLI in merito alla motivazione della sentenza della Corte Costituzionale n. 138/2010 sul matrimonio delle coppie omosessuali: "Penso sia quasi inutile sottolineare l'importanza, e direi la necessità, di una lettura evolutiva delle disposizioni costituzionali ed in particolare di quelle relative ai diritti fondamentali e inviolabili da queste desumibili e ciò senza tornare sulla nota e forse eccessivamente enfatizzata distinzione tra il carattere 'aperto' o 'chiuso' della norma espressa dall'art. 2 Cost.

Ritengo pertanto che quella espressa nella sentenza n. 138 del 2010 – per altri versi da approvare per le rilevanti affermazioni e aperture nei riguardi delle coppie omosessuali come 'formazioni sociali' costituzionalmente garantite - segni un preoccupante e poco comprensibile momento di disarmonia all'interno di una giurisprudenza costituzionale indirizzata per il resto in senso assolutamente diverso (a partire proprio dall'affermazione dell'art. 2 Cost. come norma aperta).

Come ricorda Sergio Bartole attuare la Costituzione è reiterare gli interventi nel tempo, per far sì che i principi che essa esprime trovino sempre adeguata e soddisfacente implementazione in relazione al mutare dei tempi e delle esigenze della nostra vita associata", *Corte e Diritti*, in Corte costituzionale e sistema istituzionale, Convegno dell'Associazione Gruppo di Pisa, (Pisa 4-5 giugno 2010), in corso di pubblicazione in Quaderni del Gruppo di Pisa, Giappichelli, Torino, 2011; Cfr. ancora dello stesso autore, *Per la Corte costituzionale le coppie omosessuali sono formazioni sociali, ma non possono accedere al matrimonio*, in Foro it., 2010, I, 1367 e *Il diritto "consentito" al matrimonio ed il diritto "garantito" alla vita familiare per le coppie omosessuali in una pronuncia in cui la Corte dice "troppo" e "troppo poco"*, in Giur. cost., 2010, fasc. 2.

Quanto mai attuali sembrano le osservazioni di Brandeis e Marshall: "We must never forget that it is a constitution we are expounding", vedi *supra* nota 56.

nell'art.2 cost., la garanzia del diritto alla vita privata affonda le sue radici nel terreno fertile del catalogo costituzionale."[120]

Si tenga, inoltre, presente che, ai sensi del nuovo art. 117 della Cost., l'attività legislativa dello Stato e delle Regioni deve rispettare oltre al testo costituzionale anche i vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali[121].

Ebbene, sia la tutela della vita privata sia il diritto alla protezione dei dati personali sono oggi espressamente previsti, rispettivamente negli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, la quale in virtù dell'entrata in vigore del Trattato di Lisbona ha acquisito la stessa forza dei Trattati. Anche il nuovo Trattato sul funzionamento dell'Unione europea prevede all'art 16 il diritto alla protezione dei dati personali.

Oltre a ciò, gli stessi diritti sono previsti dall'art 8 della Convenzione europea dei diritti dell'uomo, secondo l'interpretazione fornitane dalla Corte europea dei diritti dell'uomo.

Quanto al contenuto del diritto alla riservatezza, già a partire dagli anni '70 parte della dottrina, influenzata dall'esperienza statunitense, ha cominciato ad essere esteso, così, ad esempio nel 1974 Rodotà lo definiva come " la possibilità di ciascuno di controllare l'uso delle informazioni che lo riguardano"[122].

Secondo lo stesso autore, infatti, "non è più possibile considerare i problemi della privacy solo seguendo il pendolo tra riservatezza e divulgazione; tra l'uomo prigioniero dei suoi segreti e l'uomo che non ha

[120] G.ROLLA, *Il difficile equilibrio tra diritto di informazione e tutela della dignità e della vita privata: brevi considerazioni alla luce dell'esperienza italiana*, op. cit.

[121] In tale sede, sull'argomento fra i tanti si rinvia a T. F. GIUPPONI, *Corte costituzionale, obblighi internazionali e "controlimiti allargati": che tutto cambi perché tutto rimanga uguale?*, consultabile su http://www.forumcostituzionale.it/site/images/stories/pdf/documenti_forum/giurisprudenza/2007/0003_giupponi_nota_348_349_2007.pdf; D. TEGA, *Le sentenze della Corte costituzionale nn. 348 e 349 del 2007: la Cedu da fonte ordinaria a fonte "sub-costituzionale" del diritto*, consultabile in http://www.forumcostituzionale.it/site/images/stories/pdf/documenti_forum/giurisprudenza/2007/0013_tega_nota_348_349_2007.pdf; U. DE SIERVO, *Recenti sviluppi della giurisprudenza della Corte costituzionale in relazione alla giurisprudenza della Corte europea dei diritti dell'uomo*, consultabile su http://www.cortecostitu - zionale.it/informazione/ f ile/19_21_11_09_De%20Siervo_2.pdf ; E. MALFATTI, *Modelli e prassi di tutela dei diritti fondamentali, in Europa: un punto di vista italiano*, consultabile su http://joomla.ddp. unipi.it /documenti/persdoc/contributi/Elena%20Malfatti-1.pdf; Ancora vedi Corte cost. n 93/2010, consultabile su http://www.cortecostituzionale.it.. Quanto ai rapporti Stato-Regioni, in materia di trattamento dei dati personali, si segnala la sentenza della Corte Costituzionale n. 271/2005, consultabile su http://www.privacy.it/cortecost20050623.html.

[122] S. RODOTà, *La <<privacy>> tra individuo e collettività*, Pol. dir., 1974, pag. 545.

nulla da nascondere; tra la casa fortezza che glorifica la privacy e favorisce l'egocentrismo e la casa vetrina, che privilegia gli scambi sociali"[123].

La dottrina italiana, quindi, ha iniziato presto a considerare la privacy non più solo legata agli aspetti tradizionali della riservatezza, intesa cioè come diritto ad essere lasciati soli, ma anche come pretesa di controllo sui propri dati personali[124]

A questo punto, però, è necessario soffermarsi anche sull'operato della giurisprudenza, in quanto questa rappresenta un elemento particolarmente significativo, non solo per apprezzare i livelli di tutela dei diritti fondamentali raggiunti dall'ordinamento interno, ma anche nell'ottica di un possibile contributo reso all'evoluzione dei diritti, attraverso la selezione di interessi differenziati (e quindi tutelabili) che emergono all'interno della società e nei rapporti tra i consociati[125].

In Italia, in mancanza di un esplicito riconoscimento positivo del diritto privacy, prima della legge n. 675/96, il contributo giurisprudenziale alla configurazione della riservatezza/privacy come diritto e alla sua collocazione all'interno dell'ordinamento giuridico è particolarmente significativo, soprattutto ad opera della Corte di Cassazione.

I primi casi giurisprudenziali italiani relativi alla privacy risalgono agli anni 50[126] e hanno riguardato opere cinematografiche e pubblicazioni relative a vicende personali di personaggi noti, che hanno spingono gli interessati ad invocare il diritto alla riservatezza di fronte ai giudici.

Questa prima giurisprudenza ha risentito notevolmente delle divisioni dottrinali di quel tempo, relative alla tutela dell'interesse alla riservatezza, e ha riportato perciò nelle sue sentenze le medesime spaccature.

Quello che in questa sede si vuole mettere in rilievo è che, da una parte, nelle suddette decisioni la privacy è individuata nella sua "dimensione domestica"[127] e che, dall'altra parte, in quegli anni, l'interesse alla

[123] Idem, pag 547

[124] In questo senso, ad esempio A. BELVEDERE, *Riservatezza e strumenti d'informazione*, op. cit.; G.B. FERRI, *Persona e privacy*, in Riv. Dir. Comm., 1982, I.; T. E. FROSINI, *Diritto alla riservatezza e calcolatori elettronici*, in G. ALPA e M. BESSONE (a cura di), Banche-dati e diritti della persona, Cedam, Padova, 1984.

[125] E. MALFATTI, *Modelli e prassi di tutela dei diritti fondamentali, in Europa: un punto di vista italiano*, op. cit..

[126] Per un elenco delle principali sentenze dei giudici di merito dell'epoca vedi nota 152, in T. M. UBERTAZZI, *Diritto alla privacy, natura e funzioni giuridiche*, op. cit. pag 55.

[127] T. M. UBERTAZZI, *Diritto alla privacy, natura e funzioni giuridiche*, op. cit..

riservatezza è ancora una prerogativa delle persone note, più facilmente esposte, rispetto alla gente comune, ad indebite intrusioni nella propria vita privata.

Così come in America, anche in Italia la tutela della privacy è inizialmente un'esigenza avvertita solo da una parte della società.

Uno di questi casi giurisprudenziali ha riguardato due film sul tenore Enrico Caruso. Il relativo giudizio è stato promosso dai familiari del cantante defunto, i quali hanno chiesto al giudice di ordinare l'inibitoria circa la rappresentazione dei film in questione, perché ritenuti lesivi della riservatezza del congiunto.

Nella massima della sentenza, la Corte di Cassazione[128] ha manifestato un atteggiamento rivolto alla decisa negazione del diritto alla riservatezza, affermando che "nessuna disposizione di legge autorizza a ritenere che sia stato sancito come principio generale il rispetto assoluto all'intimità della vita privata e tanto meno come limite alla libertà dell'arte" e ricollegando la tutelabilità dell'interesse in questione esclusivamente al fatto che "[…] la conoscenza delle vicende della vita altrui non sia stata ottenuta con mezzi di per sé illeciti o che impongano l'obbligo del segreto […]" , attraverso cioè comportamenti che integrano gli estremi del fatto illecito.

Secondo la Cassazione, quindi, "il tema ben poteva trovare la sua soluzione, senza il bisogno di inventare istituti nuovi, nel precetto generale del 'neminem laedere', come specificato per l'appunto nell'art. 2043 c.c.".

Negli anni seguenti la Corte si è espressa in maniera sostanzialmente conforme, tornando a pronunciarsi sulla materia nel 1963[129]. La sentenza può considerarsi rilevante in quanto, pur non riconoscendo ancora il diritto alla riservatezza, segna un mutamento della rigida posizione iniziale.

La Corte, infatti, ha ribadito la mancanza di una norma che espressamente contempli la tutela della riservatezza, respingendo, inoltre, la praticabilità dello strumento analogico. Tuttavia, la stessa ha affermato l'esistenza di un "diritto erga omnes alla libertà di autodeterminazione nello

[128] Cass 22 dicembre 1956, n. 4487, in Giur. It., 1957, I, l, p.366, consultabile anche su http://www.jus.unitn.it/users/.

pascuzzi/varie/sem-inf99/cass_1956.htm.

[129] Cass. 20 aprile 1963 n. 990, in Foro it., 1963, I, p. 877, consultabile anche su http://www.jus.unitn.it/users/pascuzzi/ privcomp98-99/topics/3/Cass_1963.htm.

svolgimento della personalità dell'uomo come singolo", che trova il suo fondamento nell'art 2 della Costituzione.

"Tale diritto è violato se si divulgano notizie della vita privata, le quali, per tale loro natura, debbono ritenersi riservate, a meno che non sussista un consenso anche implicito della persona, desunto dall'attività in concreto svolta o, data la natura dell'attività medesima e del fatto divulgato, non sussista un prevalente interesse pubblico di conoscenza, che va considerato con riguardo ai menzionati doveri di solidarietà inerenti alla posizione assunta dal soggetto.

La violazione dunque della vita privata come fatto lesivo del diritto assoluto di personalità al libero svolgimento della stessa deve essere accertata con indagine da svolgersi, per singole fattispecie, sulla posizione del soggetto e sulla sussistenza di limiti, la cui inosservanza implichi illiceità e l'obbligo di risarcimento ai sensi dell'art. 2043 cod. civile."[130].

La tappa successiva nella giurisprudenza della Cassazione è rappresentata da una sentenza del 1975[131], nella quale "la formula compromissoria consacrata nella precedente decisione sembra cedere il passo alla chiara affermazione del diritto in esame."[132]

La Corte, infatti, ha posto in rilievo l'esistenza di un duplice fondamento, implicito ed esplicito, del diritto alla riservatezza: il primo è stato individuato "in quel complesso di norme ordinarie e costituzionali che, tutelando aspetti peculiari della persona, nel sistema dell'ordinamento sostanziale, non possono non riferirsi anche alla sfera privata di essa"[133].

Mentre, il fondamento definito esplicito è stato rinvenuto "in tutte quelle norme, contenute in modo particolare in leggi speciali, nelle quali si

[130] Vedi nota precedente.

[131] Cd. "caso Soraya" Cass. 27 maggio 1975, n. 2129, in Dir. aut., 1975, p. 351. Consultabile anche su http://www.jus.unitn.it/users/pascuzzi/varie/sem-inf99/Cass_1975.htm.: "tale diritto consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze, che sia pure compiute con mezzi leciti non sono giustificate da interessi pubblici preminenti." ; cfr D. FULCO, *La protezione dei dati personali. Diritti e strumenti di tutela*, in M. SGROI (a cura di) , Nuovi ambiti di tutela della personalità, Giappichelli, Torino, 2007; S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, op. cit.

[132] M. PROSPERI, *Il dibattito italiano sull'esistenza e sul fondamento del diritto alla riservatezza prima del suo espresso riconoscimento,* consultabile su http://www.privacy.it/prosperi200206.html.

[133] G. GIACOBBE, *Il diritto alla riservatezza nella prospettiva degli strumenti di tutela*, in AAVV, Il riserbo e la notizia. Atti del convegno di Studio. Macerata, 5-6 marzo 1982, Napoli, 1983, p. 113.

richiama espressamente la 'vita privata del soggetto' o addirittura la riservatezza"[134].

Inoltre, anche la Corte di Cassazione ha cominciato da abbandonare una concezione meramente domestica della privacy, estendendo il nucleo protetto dalla riservatezza a "certe manifestazioni della vita di relazione, a tutte quelle vicende, cioè, il cui carattere intimo è dato dal fatto che si svolgono in un domicilio ideale"[135].

La decisione, però, non ha adotta integralmente la concezione della privacy proposta da Rodotà, probabilmente perché nel nostro Paese non avevano ancora trovato ampia diffusione le tecnologie informatiche per il trattamento dei dati personali e la tutela della riservatezza era invocata principalmente, come visto, dalle persone più in vista nella vita pubblica[136] .

Dalla suddetta sentenza in poi la Corte non è sembrata aver mutato indirizzo, anzi, con la sentenza n. 5658/1998[137] ha fatto un ulteriore passo avanti nella ricostruzione del fondamento e del contenuto del diritto.

Infatti, dopo aver constatato come il diritto in questione è ormai riconosciuto dall'intera giurisprudenza - ricostruendone l'iter - la sentenza è passata all'analisi delle singole norme da cui si può desumere la volontà del legislatore di tutelare il riserbo e tra queste norme indica anche la L. n. 675/96, per poi affermare che "esiste un vero e proprio diritto alla riservatezza anche al di fuori delle ipotesi espressamente previste dalla legge ordinaria" e che si può inquadrare nel sistema di tutela costituzionale della persona umana, traendo fondamento in particolare dall'art. 2 Cost..

In particolare, la Corte ha inteso tale articolo nella sua più ampia dimensione di clausola generale, "aperta all'evoluzione dell'ordinamento suscettibile, per ciò appunto, di apprestare copertura costituzionale ai nuovi valori emergenti della personalità, in correlazione anche all'obbiettivo primario di tutela 'del pieno sviluppo della persona umana' [...]".

La vicenda che, invece, ha portato all'attenzione della Cassazione la riservatezza, nella sua dimensione moderna di controllo della circolazione

[134] G.GIACOBBE, *Il diritto alla riservatezza nella prospettiva degli strumenti di tutela* , op. cit.;

[135] G. FAMIGLIETTI, *Il diritto alla riservatezza o la riservatezza come diritto. Appunti in tema di riservatezza ed intimidad sulla scorta della giurisprudenza della Corte costituzionale e del Tribunal Constitucional*, consultabile su http://www.forumcostituzionale.it/site/index3.php?option=content&task=view&id=212.

[136] T. M. UBERTAZZI, in Diritto alla privacy, natura e funzioni giuridiche, op. cit.; T. A. AULETTA, Riservatezza e tutela della personalità, op. cit., pag 64.

[137] Consultabile su www.diritto-civile.it/.../Cass-civ-sez.-III-n.-5658-del-1998.html

dei propri dati personali, è quella definita con la sent. n. 8889/2001[138] (il caso della Vedova Olcese).

In essa, la Suprema Corte ha rilevato che la portata della legge n. 675 del 1996 non è limitata all'archiviazione delle informazioni nelle banche dati, ma a qualunque trattamento, anche quello giornalistico, dell'informazione. Quindi, non è solo il trattamento diretto alla conservazione in archivio a dover essere svolto nel rispetto dei principi stabiliti dall'art. 1 della legge n. 675 del 1996, a tutela dei diritti fondamentali e della dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale.

Quanto agli interventi della Corte Costituzionale, questi, invece, sono stati essenzialmente sporadici, non avendo avuto occasione di affrontare il problema dell'esistenza di un diritto alla riservatezza come tema generale, ma solo in relazione ad aspetti settoriali.

Ciò è stato determinato probabilmente sia alla mancanza nel testo costituzionale di un riferimento esplicito a tale diritto sia all'assenza, fino a tempi piuttosto recenti, di norme di grado primario a tutela della privacy che potessero essere portate alla sua attenzione.

Infatti, sebbene esistano precedenti affermazioni del diritto in questione[139], è stato solo con la pronuncia n. 38 del 1973 che la Corte, nel riconoscere la tutela dei diritti inviolabili dell'uomo per il pieno sviluppo della persona e della libertà, ai sensi dell'art. 2, dell'art. 3, 2° comma, dell'art. 13, 1° comma, Cost., ha affermato che fra questi "rientra quello al proprio decoro, del proprio onore, della propria rispettabilità, riservatezza e intimità e reputazione"[140].

---

[138] Corte Cass. I sez, civile, consultabile su http://www.privacy.it/cassaz20010630.html . La questione riguardava la rivendicazione, da parte della seconda moglie di un noto industriale deceduto, del cognome del marito, con il quale negli articoli del quotidiano, Il Corriere della Sera, si continuava ad indicare la prima moglie, nonostante il matrimonio fosse stato annullato dalla Sacra Rota. La donna si era rivolta al Garante per la privacy, il quale aveva ordinato la rettifica degli articoli in questione, ma il direttore del quotidiano milanese si era opposto davanti al Tribunale di Milano, sostenendo che tale ordine non rientrava tra i poteri dell'Autorità Garante. L'opposizione veniva accolta e per questo la signora era ricorsa in Cassazione. La Cassazione ha accolto il ricorso e, decidendo nel merito, ha rigettato l'opposizione proposta dalla RCS Editori S.p.A. contro il provvedimento dell'Autorità garante.

[139] Un primo riconoscimento- nella giurisprudenza costituzionale – del diritto alla riservatezza, è stato individuato – vedi G. FAMIGLIETTI, *Il diritto alla riservatezza o la riservatezza come diritto. Appunti in tema di riservatezza ed intimidad sulla scorta della giurisprudenza della Corte costituzionale e del Tribunal Constitucional*, op cit; G.CASSANO, *il diritto alla riservatezza fra dottrina e giurisprudenza*, in studiocelentano.it - nella sentenza n 122/1970 in cui si tratta del diritto d'autore, del diritto all'immagine, in rapporto all'art. 21 e nella sentenza 12/1972, in tema di questue, in cui la Corte riconosce un generale diritto a non rivelare le proprie convinzioni. Sentenza consultabili su http://www.cortecostituzionale.it/

[140] Corte costituzionale n 38/73 consultabile su http://www.giurcost.org/decisioni/1973/0038s-73.html.

Seppur incidentalmente e inserendolo in elenco più ampio, con questa pronuncia la Corte ha riconosciuto, quindi, il diritto alla riservatezza e ne ha rinvenuto il fondamento costituzionale attraverso l'interpretazione dell'art. 2, non tanto come "clausola aperta", fonte autonoma di diritti a sé stanti e non deducibili da altre parti della Carta, quanto piuttosto come sostegno qualificatore rispetto a diritti o principi pur non espressi, ma riconducibili anche in via implicita ad altre norme costituzionali[141].

Questo pare essere il cammino intrapreso dalla Corte Costituzionale e sostanzialmente mai abbandonato, ossia quello della ricerca di una soluzione aderente ed in linea con i valori costituzionali a protezione della persona, affiancando alla protezione dell'elemento materiale e personale da ingerenze ingiustificate esterne, uno più ampio, quello del patrimonio psicologico da difendere per un libero e consapevole sviluppo della personalità[142].

Questo cammino è ispirato, in generale, ad un criterio di ragionevole bilanciamento dei diversi interessi contrapposti[143].

---

[141] G. FAMIGLIETTI, *Il diritto alla riservatezza o la riservatezza come diritto. Appunti in tema di riservatezza ed intimidad sulla scorta della giurisprudenza della Corte costituzionale e del Tribunal Constitucional*, op cit; Per una lettura della sentenza in chiave di interpretazione dell'art. 2 cost. come clausola aperta, vedi M. PROSPERI, *Il diritto alla riservatezza nell'ordinamento costituzionale*, op. cit..

[142] Vedi fra le altre Corte cos. n. 366/91, in Giur. cost., 1991, p. 2914 ss, consultabile su http://www.giurcost.org/decisioni/1991/0366s-91.html - in tema di diritto alla libertà e segretezza della corrispondenza, in cui i giudici ritengono che: "La stretta attinenza di tale diritto al nucleo essenziale dei valori di personalità -che inducono a qualificarlo come parte necessaria di quello spazio vitale che circonda la persona e senza il quale questa non può esistere e svilupparsi in armonia con i postulati della dignità umana- comporta una duplice caratterizzazione della sua inviolabilità. In base all'art. 2 della Costituzione, il diritto a una comunicazione libera e segreta e inviolabile, nel senso generale che il suo contenuto essenziale non può essere oggetto di revisione costituzionale, in quanto incorpora un valore della personalità avente un carattere fondante rispetto al sistema democratico voluto dal Costituente. In base all'art. 15 della Costituzione, lo stesso diritto é inviolabile nel senso che il suo contenuto di valore non può subire restrizioni o limitazioni da alcuno dei poteri costituiti se non in ragione dell'inderogabile soddisfacimento di un interesse pubblico primario costituzionalmente rilevante, sempreché l'intervento limitativo posto in essere sia strettamente necessario alla tutela di quell'interesse e sia rispettata la duplice garanzia che la disciplina prevista risponda ai requisiti propri della riserva assoluta di legge e la misura limitativa sia disposta con atto motivato dell'autorità giudiziaria."

La giurisprudenza costituzionale ha ravvisato, quindi, nella riservatezza una componente della dignità umana e del rispetto della personalità individuale (vedi anche sent. 471/1990, in *Giur. cost*., 1990, p. 2818 ss.; 257/1996, in Giur. cost., 1996, p. 2306 ss.) e, allo stesso tempo, un fattore di promozione umana che consente il pieno ed effettivo esercizio di altri diritti fondamentali (sent. 139/1990, cit.). In ordine a quest'ultima interpretazione che la Corte dà al legame fra diritto alla riservatezza e dignità umana, G. TIBERI, *Riservatezza e protezione dei dati personali*, in M. CARTABIA (a cura), I diritti in azione, op cit., p.359 sottolinea, tuttavia, che tale profilo appare ancora solamente sfiorato dal Giudice delle leggi,rimanendo "assai sfumate nei loro contorni (…) le tracce di una dimensione positiva della riservatezza".Al contrario, l' Autrice rileva come di un vero e proprio "diritto allo sviluppo personale" collegato alla riservatezza della sfera privata parli la Corte europea dei diritti dell'uomo nella sent. 6 febbraio 2001,*Bensaid*, par. 47

[143] Vedi ad esempio sent n. 372/06, consultabile su http://www.cortecostituzionale.it, in cui si legge: "Lo scrutinio di costituzionalità non deve essere effettuato in astratto, tra i valori in sé e per sé considerati, ma in concreto, valutando l'interazione reciproca tra l'accrescimento di tutela dell'uno e la corrispondente diminuzione di garanzia dell'altro, come disposti dal legislatore in vista della composizione del potenziale

Quanto ai primi interventi della Corte su problematiche inerenti alla privacy, intesa con controllo sulla circolazione dei propri dai personali, si segnala la sentenza n 81 del 1993[144], in cui la Corte ha affermato che "il riconoscimento e la garanzia costituzionale della libertà e della segretezza della comunicazione comportano l'assicurazione che il soggetto titolare del corrispondente diritto possa liberamente scegliere il mezzo di corrispondenza, anche in rapporto ai diversi requisiti di riservatezza che questo assicura sia sotto il profilo tecnico, sia sotto quello giuridico (….)". Pertanto, "va riconosciuto il diritto di mantenere segreti tanto i dati che possano portare all'identificazione dei soggetti della conversazione, quanto quelli relativi al tempo e al luogo dell'intercorsa comunicazione".

Si veda ancora la sentenza n. 463 del 94, in cui si legge che: "La decisione giudiziale sulla richiesta, da chiunque formulata, relativa alla distruzione del materiale documentale attinente a intercettazioni telefoniche incide in ogni caso sopra un diritto costituzionale - quello alla riservatezza delle proprie comunicazioni - che è stato dichiarato più volte da questa Corte come un diritto inviolabile ai sensi dell'art. 2 della Costituzione e, in quanto tale, restringibile dall'autorità giudiziaria soltanto nella misura strettamente necessaria alle esigenze di indagine legate al compito primario concernente la repressione dei reati (v. sent. nn. 63 del 1994, 81 del 1993, 366 del 1991 e 34 del 1973)."[145]

Così sì e espressa anche più recentemente la sentenza 372 del 2006, in cui la Corte ha parlato di "principio costituzionale della tutela della riservatezza dei dati relativi alle comunicazioni telefoniche"[146]

---

contrasto." Ancora, recentemente, vedi sent n. 173/09, consultabile su http://www.cortecostituzionale.it , in cui si legge: "D'altra parte, la pressante esigenza di dare al diritto fondamentale alla riservatezza una tutela più intensa, rispetto a quella, rivelatasi insufficiente, del recente passato, induce a ritenere non irragionevoli particolari modalità di trattamento del materiale probatorio, che riescano a contemperare tutti i diritti e principi fondamentali coinvolti in questa delicata materia. Le modalità di bilanciamento tra i suddetti diritti e principi sono molteplici e non spetta a questa Corte, ma al legislatore, individuare possibili soluzioni nell'ambito della disciplina del processo penale. Nel presente giudizio le valutazioni che il giudice delle leggi è chiamato ad esprimere sono necessariamente limitate dall'oggetto della questione ed in questa cornice deve essere ricercato il punto di equilibrio tra le diverse e potenzialmente opposte esigenze, tutte costituzionalmente protette, che vengono in rilievo. Diversi e migliori equilibri possono essere individuati dal legislatore – dotato di poteri innovativi non istituzionalmente attribuiti a questa Corte – nel rispetto dei diritti e dei principi evocati nel presente giudizio."

[144] Consultabile su http://www.giurcost.org/decisioni/1993/0081s-93.html

[145] Corte cost. 463/94 consultabile su http://www.giurcost.org/decisioni/1994/0463s-94.html

[146] Corte cost. 372/06, consultabile su http://www.cortecostituzionale.it

3.1. Principali fonti legislative nazionali

Come già messo in evidenza, in Italia è mancata per molto tempo una norma che definisse e tutelasse la riservatezza ed i dati personali, pur esistendo un mosaico di disposizioni che proteggevano "l'area della vita privata"[147]

Al riguardo, l'art. 8 dello Statuto dei lavoratori del 1970, il quale vieta la raccolta delle opinioni politiche, sindacali e religiose dei dipendenti, è considerato l'atto di nascita in Italia della protezione dei dati personali. Ciò con l'evidente paradosso per cui quello che era stato definito un diritto tipico della borghesia entra nell'ordinamento giuridico positivo italiano con una legge volta alla tutela dei lavoratori [148].

Anche nel nostro Paese, però, negli anni 80 hanno cominciato a svilupparsi le banche dati informatiche e l'utilizzo della tecnologia su scala non elitaria, ma di massa, tanto che la dottrina ha iniziato a ritenere quasi realistici gli scenari fantastici descritti da Orwell [149]. Si è iniziato, perciò, ad avere coscienza sempre di più che le tecnologie informatiche sono in grado di muovere un numero incredibile di informazioni, sottoponendo il cittadino ad una nuova forma di dominio sociale: il potere informatico[150].

Tuttavia, mentre in quegli anni, in Europa alcuni stati hanno già cominciano ad emanare leggi a tutela della privacy[151] e nel 1981 è stata

[147] Si pensi all'art 10 c.c. sul diritto di immagine, all'art 21 e all'art.24 della legge sul diritto d'autore, riguardo l'anonimato e l'inedito, l'art 595, 2c c.p., sulla difesa dell'onore contro la rivelazione di fatti determinati, all'art 614, sull'inviolabilità del domicilio e all'art 616 c.p., sull'inviolabilità della corrispondenza.

[148] Così S NIGER, *Le nuove dimensioni della privacy*, op cit. pag 52; Vedi S. RODOTà, *La <<privacy >> tra individuo e collettività,*op. cit.. Si veda anche quanto descritto da B. GUIDETTI SERRA nel libro *Le schedature Fiat*, Rosenberg & Sellier, 1984. Per una lettura diversa si veda ad esempio, T.M. UBERTAZZI, *in Diritto alla privacy, natura e funzioni giuridiche*, op. cit., il quale osserva che: "Mi sembra che al momento dell'emanazione dello statuto dei lavoratori fosse avvertita in Italia non tanto la 'paura della schedatura' (…) quanto la 'paura' della discriminazione. (…). La pretesa alla riservatezza, e mi ripeto, riguardava infatti ancora alla fine degli anni 70 persone note riprese con il teleobiettivo e non era ancora avvertita come interesse da proteggere del *quisque de popolo*. Sicuramente l'art.8 è stato nel corso degli anni applicato alla tutela del diritto alla riservatezza, o meglio di un suo aspetto particolare, ma mi sembra implausibile sostenere che il legislatore abbai previsto la norma dello statuto con il preciso e principale obiettivo di tutelare la privacy del lavoratore dipendente. In quest'ottica mi sembra, inoltre, che lo statuto dei lavoratori ha per lo più dimostrato che il suo intento non era tanto di conferire un potere di controllo al lavoratore sui propri dati personali quanto invece di rendere effettivo un controllo sulla posizione contrattuale 'forte' del datore di lavoro".

[149] V S. RODOTà *Elaboratori elettronici e controllo sociale*, il Mulino, Bologna,1973 ; G.B. FERRI, *Persona e privacy*, op. cit.; T. M. UBERTAZZI, *Diritto alla privacy, natura e funzioni giuridiche*, op. cit.; S. NIGER, *Le nuove dimensioni della privacy* op. cit.

[150] S.NIGER,*Le nuove dimensioni della privacy*, op. cit.

[151] Ad esempio, in Francia la Loi n 78-17 del 1978 relativa a l'informatique, aux fichiers et auw liberties o nel Regno Unito il Data protection Act emanato nel 1984.

adottata a Strasburgo dal Consiglio d'Europa la "Convenzione per la protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale" n. 108, entrata in vigore a partire dal 1 ottobre 1985[152], in Italia, invece, tutte le diverse proposte di legge, aventi lo scopo di regolare in maniere completa il diritto alla riservatezza non sono state approvate[153]

La legge 31 dicembre 1996, n. 675 – *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali* – ha rappresentato, così, la prima legge organica sulla tutela dei dati personali nel nostro ordinamento.

Tale legge frutto, come si è visto, di un lungo dibattito parlamentare e di una lunga elaborazione dottrinale, ha recepito i principi della Convenzione n. 108 di Strasburgo e della Direttiva comunitaria 95/46/Ce.

Adottata in adempimento della suddetta direttiva comunitaria e degli obblighi derivanti dal Trattato di Schengen[154], la normativa italiana ne ha allargato però in modo significativo l'ambito di applicazione, con l'esplicito riferimento nell'art. 1 alla tutela della dignità delle persone fisiche e all'identità personale, nonché con l'estensione della tutela anche ai trattamenti non organizzati in banche dati e ai dati delle persone giuridiche[155].

L'art. 1 della legge ha individuato, infatti, l'obiettivo della disciplina nel far sì che il trattamento dei dati personali si svolga "nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale" garantendo anche "i diritti delle persone giuridiche e di ogni altro ente o associazione".

In questo modo, l'oggetto della tutela non è stato limitato al diritto di ciascuno ad esigere che i trattamenti automatizzati dei suoi dati personali avvengano nel rispetto di regole e principi, ma ha finito per interessare una parte rilevante dei cd. diritti della personalità.

---

[152] Consultabile su http://www.governo.it/GovernoInforma/Dossier/social_network/108.pdf .

[153] Es. i progetti Accade (presentato il 21 aprile 1981), Picano (presentato il 24 febbraio 1982), Mirabelli (presentato il presentato il 20 luglio 1982), Martinazzoli (presentato il 4 maggio 1984), Bozzi (presentato il 29 gennaio 1985- questo progetto prevedeva l'introduzione nel testo costituzionale degli artt 21 bis e 21 ter. In particolare, l'art. 21 bis recitava che "nei limiti e nei modi stabiliti dalla legge, tutti hanno diritto di cercare, trasmettere e ricevere informazioni, nonché di accedere ai documenti e agli atti amministrativi che lo riguardano. Sono vietati la raccolta e l'uso di informazioni che implicano discriminazioni o lesioni dei diritti fondamentali della persona".

[154] l'Europa avrebbe permesso di godere dei benefici dell'Accordo di Schengen solo se il paese membro avesse adeguato la normativa sul trattamento dei dati personali.

[155] M. SGROI, (a cura di) , *Nuovi ambiti di tutela della personalità*, op.cit.

Nella legge n. 675/96, pertanto, la riservatezza si presenta come uno soltanto dei diritti presi in considerazione, "come una specificazione in un quadro connotato dalla esplicita rilevanza attribuita al complesso dei diritti e delle libertà fondamentali. Una lettura condotta solamente in termini di privacy porterebbe a un'impropria ricostruzione di questo stesso concetto, che va inteso nella più larga dimensione fatta propria dal legislatore italiano"[156].

Inoltre, con la suddetta legge è stato positivizzato l'aspetto dinamico assunto dalla privacy nella società dell'informazione, ovvero l'autodeterminazione informativa. E' stata, infatti, disciplinata la possibilità di accedere alle informazioni che riguardano la propria persona, al fine di controllare la correttezza della loro acquisizione, correggere gli eventuali errori e sorvegliarne l'impiego nel corso del tempo.

In seguito, in virtù della legge delega n. 127/2001, è stato adottato il D.lgs. n. 196/03, *Codice in materia di protezione dei dati personali*[157].

Pur non contenendo norme regolamentari (non è un Testo Unico cd. misto), il decreto è andato oltre la ricognizione compilativa delle disposizioni legislative vigenti, operando una riorganizzazione completa del materiale normativo, finalizzata ad una maggiore coerenza e ad un rafforzamento di tutela, anche alla luce delle successive direttive comunitarie, dei principi elaborati dalla dottrina, delle interpretazioni operate dalla giurisprudenza e dal Garante per la protezione dei dati personali, istituito con la precedente legge n. 675/96.

Il nuovo Codice, in virtù della materia che mal si presta a discipline troppo rigide e definite, ha come caratteristica fondamentale, anche criticata come si vedrà, quella di fornire appunto una cornice normativa di principi e di indirizzi, lasciando la regolamentazione concreta e specifica ai provvedimenti dell'Autorità garante.

Inoltre, nonostante il mancato inserimento delle norme regolamentari, la previsione di un disciplinare tecnico per le cd misure minime di sicurezza, così come l'allegazione degli esistenti codici di deontologia e di buona condotta, nonché la previsione dell'inserimento automatico di quelli che

[156] S. NIGER, *Le nuove dimensioni della privacy*., pag 111.

[157] Consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1311248

verranno successivamente adottati[158], hanno consentito di ritenere, comunque, il Testo Unico uno strumento agile e sufficientemente completo, il primo modello in ambito europeo di codificazione organica in materia.

Il Codice si compone di tre parti, contenenti rispettivamente: le disposizioni generali, concernenti le regole sostanziali della disciplina del trattamento dei dati personali, applicabili a tutti i trattamenti, salvo eventuali regole specifiche per i trattamenti effettuati da soggetti pubblici e privati; le disposizioni particolari per specifici trattamenti, ad integrazione o eccezione delle disposizioni generali; le disposizioni relative alle azioni di tutela dell'interessato e al sistema sanzionatorio.

Il nuovo Codice ha assegnato un rilevo maggiore ai diritti e alle libertà fondamentali[159], riconoscendo per la prima volta espressamente un diritto alla protezione dei dati personali. Ciò, si ripete, ha valorizzato l'aspetto dinamico che è venuto a caratterizzare il concetto di privacy, con lo sviluppo preponderante delle nuove tecnologie: dalla tradizionale tutela del riserbo all'attribuzione all'interessato del diritto all'autodeterminazione informativa[160].

Mentre la legge n. 675 del 1996 poneva al centro del sistema normativo gli adempimenti formali dell'informativa del consenso, della notifica al Garante e le stesse modalità di esercizio dei diritti, il nuovo Codice ha privilegiato gli aspetti di garanzia della persona, assegnando un ruolo prevalente al procedimento di "trattamento", alle situazioni soggettive da

[158] L'osservanza sia delle norme sulle cd. misure minime di sicurezza sia di quelle autonomamente datasi dalla categorie professionali, costituiscono condizione necessaria per determinare la liceità del trattamento dei dati personali. Vedi G.P. CIRILLO, *Il nuovo codice in materia di trattamento dei dati e gli schemi di riferimento relativi alla tutela dei diritti fondamentali della persona e dei cd. diritti dell'interessato*, in G. SANTANIELLO (a cura di), La protezione dei dati personali, Cedam, Padova, 2005.

[159] G. P. CIRILLO, *Il nuovo codice in materia di trattamento dei dati e gli schemi di riferimento relativi alla tutela dei diritti fondamentali della persona e dei cd. diritti dell'interessato*, op. cit; S. NIGER, *Le nuove dimensioni della privacy*, op. cit.; M. SGROI, (a cura di) , *Nuovi ambiti di tutela della personalità*, op. cit.

[160]Si è già evidenziato come l'autonomia concettuale del diritto alla protezione dei dati personali era sta già riconosciuta nella Carte dei diritti fondamentali dell'Unione europea (art 8). Come ha osservato S. RODOTà, la costruzione di un *habeas data* prende le mosse proprio dal diritto di controllare l'uso che altri facciano delle informazioni che lo riguardano: "La libertà personale non è difesa soltanto attraverso il diritto di essere lasciato solo, secondo la definizione che racchiude la più antica essenza della privacy e che si concreta nel potere di impedire la circolazione dei dati personali. Diviene un potere di controllo sull'esterno, sia per mantenere l'integrità di sé seguendo on ogni momento i dati diffusi nell'ambiente, sia per impedire la violazione della propria sfera privata attraverso informazioni non gradite. Il controllo sulle informazioni in entrata, strutturato in un più generale <<diritto di non sapere>>, diventa un momento caratterizzante della nuova definizione della privacy e incarna quel momento di intangibilità del corpo e di divieto sue invasioni cha appartiene alla più antica tradizione dell'*habeas corpus*" . S. RODOTà, *Libertà personale. Vecchi e nuovi nemici*, in M. BOVERO (a curadi), Quale libertà. Dizionario contro i falsi liberali, Laterza, Roma-Bari, 2004, pag 52; Vedi anche S. NIGER, *Le nuove dimensioni della*, op. cit.

questo generate e i rimedi contro le "devianze" rispetto alle regole prefissate.

Non è un caso, quindi, che la Parte I del Codice abbia posto subito in primo piano i diritti e le libertà fondamentali degli interessati e collochi, invece, gli obblighi di tipo formale e procedurale nella Parte II.

In tal senso, viene in rilievo la positivizzazione del principio secondo cui la disciplina del trattamento dei dati personali deve garantire un livello *elevato* di tutela dei diritti e delle libertà fondamentali dell'interessato (art. 2, comma 2). Tale principio che deve orientare sia le normative regolamentari, sia le discipline dei diversi codici di deontologia, così come qualunque operatore si trovi ad applicare il Codice, ivi compresi il Garante e i giudici.

La nuova disciplina ha arricchito l'elenco delle definizioni contenuto nella legge n. 675/09, aggiungendo nozioni, come quella dei dati identificativi o quella dei dati giudiziari[161], ovvero chiarendo nozioni già

[161] Art. 4. Definizioni (consultabile integralmente su http://www.garanteprivacy.it/garante/doc.jsp?ID=1311248)

1. Ai fini del presente codice si intende per:

a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;

d) "dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

e) "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R.. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

f) "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g) "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

l) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

m) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

indicate, ma con opportune precisazioni (es. la definizione di banca dati). Inoltre ha semplificato sia gli adempimenti a carico delle imprese e delle pubbliche amministrazioni, sia le modalità di esercizio dei diritti.

Si segnala, inoltre, che il Codice, sotto l'impronta della direttiva 2002/58/CE[162], contiene un'importante innovazione all'articolo 3, introducendo il principio di necessità: "i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione dei dati personali e dei dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettono di identificare l'interessato solo in caso di necessità" [163].

L'inserimento di tale principio ha corrisposto anche alla crescente importanza del principio di precauzione, al quale fa riferimento l'articolo 174 del Trattato dell'Unione europea[164], attualmente enunciato all'art. 191 del Trattato sul funzionamento dell'Unione europea.

Sempre riguardo alle maggiori innovazioni previste del Codice, si evidenzia il principio sancito dall'art 11 comma 2[165], secondo il quale i dati

n) "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

o) "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

p) "banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

q) "Garante", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

(…)

[162] Direttiva 2002/58/CE, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=35284. Il principio è presente anche nella legislazione tedesca, art 3 – Parsimonia e misura nell'utilizzo dei dati personali – del Federal Data Protection Act (Bundesdatenshutzgesetz), adottato il 18 maggio 2001.

[163] "Il principio di necessità contribuisce a laicizzare il rapporto tra l'innovazione scientifica e la società.", cosi S. RODOTà, *Laicizzare il rapporto fra innovazione e società, in Innovazioni tecnologiche e privacy*, op. cit.

[164] L'Unione Europea ha recepito il principio nel trattato in materia di protezione ambientale, tuttavia, nella pratica, nei documenti di orientamento politico e nelle sentenze della Corte di Giustizia il campo d'applicazione del principio è molto più vasto e si estende anche alla politica dei consumatori e alla salute umana, animale o vegetale.

Per questi motivi, il Consiglio, nella sua risoluzione del 13 aprile 1999, ha chiesto alla Commissione di elaborare degli orientamenti chiari ed efficaci al fine dell'applicazione di detto principio. Da qui la "Comunicazione della Commissione sul principio di precauzione" del 2 febbraio 2000, sul ricorso al principio di precauzione. Vedi http://europa.eu/legislation_summaries/consumers/consumer_safety/l32042_it.htm

[165] Art. 11. Modalità del trattamento e requisiti dei dati

1. I dati personali oggetto di trattamento sono:

a) trattati in modo lecito e secondo correttezza;

b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;

c) esatti e, se necessario, aggiornati;

trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Per comprendere la portata di tale previsione, è necessario considerare che prima dell'introduzione del Codice, gli interventi inibitori disposti prevalentemente in via amministrativa dal Garante (oltre ai pochi casi presso la giurisdizione civile o penale in materia di provvedimenti di sequestro penale) hanno avuto come scopo per lo più quello di interrompere le condotte illecite e di ordinare, ad esempio, di astenersi dal proseguire il trattamento in violazione di legge.

Così, seppur in alcuni casi è stata accolta, in tutto o in parte, la specifica istanza dell'interessato, ai sensi dell'art 13 della legge n. 675/96, volta a cancellare i dati trattati con effetto *ex nunc*, nella maggioranza delle situazioni il Garante ha fatto piuttosto uso del potere di "segnalazione"[166], d'ufficio o su istanza di parte o reclamo, accertando un'inosservanza di legge, senza adottare un provvedimento inibitorio con conseguenze dirette sulla sorte dei dati personali indebitamente trattati.

La figura dell'inutilizzabilità, quindi, ha rivisto molto il sistema di protezione dei dati, perché fa seguire all'illecito trattamento la conseguenza giuridica forse più significativa[167], con effetto, tra l'altro, insanabile.

Altri principi rilevanti, sanciti sempre dall'art 11 del Codice, riguardano il principio di liceità e correttezza del trattamento[168]e, soprattutto, il principio di finalità. La raccolta dei dati deve avvenire, infatti, per uno o più scopi o finalità determinate, esplicite e legittime.

Tale principio costituisce un forte strumento di controllo per la circolazione dell'informazione, consentendo all'interessato di esercitare in modo più efficace il controllo sul flusso dei propri dati personali.

Questo, poi, "si traduce nella manifestazione di un consenso, ove previsto, libero e informato e nel diritto alla cancellazione, rettificazione o

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

166 Art 31, comma 1 della legge n. 675/96.

167 L'inutilizzabilità è prevista in sede pensale per le fonti di prova acquisite in violazione dei divieti di legge (art 191 c.p.p.).

168 Vedi S. NIGER, *Le nuove dimensioni della privacy*, op. cit., pag 134.

integrazione dei dati. Il principio di trasparenza, inoltre consente di valutare in modo più analitico la pertinenza dei dati rispetto agli scopi prefissati, nonché il periodo di necessaria conservazione degli stessi."[169].

Superato tale periodo, infatti, i dati devono essere cancellati o trasformati in forma anonima, garantendo così il diritto all'oblio dell'interessato[170].

I principi stabiliti dall'art 11 del Codice, vanno letti alla luce soprattutto di quanto previsto dall'art 7, comma 3, lett. b), relativo appunto al diritto dell'interessato di chiedere al titolare del trattamento la cancellazione o la trasformazione in forma anonima delle sue informazioni personali, se trattate in violazione di legge o se non è più necessaria la conservazione in base agli scopi perseguiti.

Altro principio fondamentale nell'ambito della normativa sul trattamento dei dati personali è quello del consenso. L'art. 23 del Codice, comma 1, riprendendo l'art 11 della L. n. 675/96, prevede che il trattamento dei dai personali da parte di privati ed enti pubblici sia ammesso solo con il consenso espresso dell'interessato[171].

Tuttavia, il legislatore ha evitato di assegnare al consenso un primato assoluto[172], pur costruendo intorno a questo un complesso di garanzie e prerogative, "in coerenza con la scelta del legislatore di abbandonare un modello di tutela passiva (divieti) a favore di un insieme di strumenti di difesa attiva (informazione, consenso, accesso)"[173].

L'importanza del consenso nella regolazione del trattamento dei dati personali ha confermato, inoltre, la centralità della libera scelta e del potere decisionale dell'interessato nella materia dei diritti fondamentali[174]. Il diritto

[169] S. MELCHIONNA, in R. ACCIAI (a cura di), *Il diritto alla protezione dei dati personali: la disciplina sulla privacy alla luce del nuovo Codice*, Maggioli, Rimini, 2004, pg 70.

[170] Sul tema: G.B. FERRI, *Diritto all'informazione e diritto all'oblio*, in "Rivista di diritto civile", 1990; M. MEZZANOTTE, *il Diritto all'oblio vs diritto alla memoria: il moderno sviluppo della privacy*, in "Diritto pubblico comparato ed europeo", 2002; G. CASSANO, *Il diritto all'oblio esiste: è diritto alla riservatezza* (nota a Trib. Roma 15 maggio 2005), in Il diritto di famiglia e delle persone, 1998.

[171] S. RODOTà, "…Questa rinnovata preferenza per il consenso si spiega con le difficoltà o le diffidenze, relative alla possibilità di mettere a punto un completo sistema di autorizzazioni e divieti in via legislativa. Il consenso, in tal modo, appare una via di mezzo tra regulation e deregulation", in *Tecnologia e diritti*, op. cit., pag 81.

[172] S. RODOTà, *Tecnologia e diritti*, op cit., in caso contrario "verrebbe completamente trascurata l'altra dimensione, legata alle conseguenze sociali ad alle conseguenze per lo stesso interessato, della circolazione di determinate informazioni personali e di informazioni raccolte per determinate finalità" pag 82, "Non è possibile affidarsi unicamente alle decisioni individuali, anche se alla base di queste si richiede il consenso informato" pag. 220.

[173] S. MELCHIONNA, in R. ACCIAI (a cura di), *Il diritto alla protezione dei dati personali: la disciplina sulla privacy alla luce del nuovo Codic,e* op. cit., p 119.

[174] S. PATTI, *Il consenso dell'interessato al trattamento dei dati personali*, in Rivista di diritto civile, 1999.

all'autodeterminazione informativa dell'interessato si fonda proprio sulla concezione del consenso al trattamento dei dati personali[175].

Una volta prestato il consenso, inoltre, non si estingue il rapporto fra il soggetto e le proprie informazioni; il soggetto interessato, infatti, conserva un potere di controllo sulle modalità del trattamento stesso.

Oltre ai rimedi previsti dall'art 7 del Codice, lo strumento che consente al soggetto interessato di riappropriarsi del potere di controllo sulla circolazione delle proprie informazioni è individuato anche dalla revoca del consenso, inteso come strumento di "recupero della sovranità su se stessi"[176].

Anche se la revocabilità del consenso non è prevista esplicitamente, in quanto la legge ha considerato solo l'opposizione per motivi legittimi[177], tuttavia, la dottrina ne ha ammesso la sostanziale esistenza: alcuni in base alla natura giuridica del consenso e alla sua riconducibilità alla disponibilità dell'avente diritto, altri, invece, riconducendola alla funzione del consenso, ovvero quella di consentire al soggetto di esprimere la propria personalità individuale.

Il fondamento della revoca andrebbe, quindi, ricercato in quello stesso potere di autodeterminazione del soggetto che nella manifestazione del consenso aveva trovato il suo primo e principale atto di esercizio[178].

In ogni caso, anche l'esercizio del potere di revoca dovrà conformarsi ai canoni della buona fede e della correttezza[179].

Ai sensi dell'art 23, comma 3 del Codice, il consenso si intende validamente prestato "solo se è espresso liberamente e specificatamente in riferimento ad un trattamento chiaramente individuato, se è documentato

175 E' accesa la questione fra i sostenitori della tesi negoziale del consenso (Oppo, Zeno Zencovich) e quanti, invece, ne rinvengono natura non negoziale, ma autorizzativa (Patti, Messinetti, Viciani, Resta)

176 S. RODOTà, *Persona, riservatezza, identità,*op. cit., pag 590.

177 La legge spagnola del 1992, invece, disciplina esplicitamente la revoca del consenso per giusta causa, si veda M G. LOSANO, *La legge spagnola sulla protezione dei dati personali*, in Il diritto dell'informazione e dell'informatica, 1993.

178 In questo senso G. RESTA, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in Rivista critica del diritto privato, pp. 310 e ss. S. PATTI, richiama l'attenzione sulla necessità di distinguere le ipotesi in cui il trattamento non si ancora iniziato, nel qual caso la revoca non dovrebbe incontrare alcun limite, dalle ipotesi in cui il trattamento sia già avviato, in cui assume rilevanza anche l'interesse di chi ha ottenuto il consenso allo svolgimento dell'attività, in Il consenso dell'interessato al trattamento dei dati personali, *Il consenso dell'interessato al trattamento dei dati personali,* op cit., pag 465.

179 G. RESTA, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali* , op. cit., pag 311.

per iscritto, e se sono state rese all'interessato le informazioni di cui all'art. 13".

Come osservato dal Garante per la protezione dei dati personali[180], il consenso può essere ritenuto effettivamente libero solo se si presenta come manifestazione del diritto all'autodeterminazione informativa, al riparo, quindi, da qualsiasi pressione o condizionamento all'accettazione di clausole che determinano un significativo squilibrio dei diritti e degli obblighi di un contratto.

Il consenso, infine, deve essere informato. L'informazione del soggetto chiamato a manifestare il suo consenso diventa condizione imprescindibile per garantirne l'effettività.

La nuova disciplina ha previsto, inoltre, all'art 12, l'emanazione di codici deontologici di autoregolamentazione delle singole categorie professionali, imprenditoriali e degli enti pubblici. Questi codici sono promossi dal Garante ed elaborati in coordinamento fra gli interessati e lo stesso Garante, al fine di affiancare alla normativa anche una disciplina partecipata[181]. La liceità e la correttezza del trattamento dei dati personali dipendono anche dal rispetto di questi codici.

Nell'ambito del sistema di garanzie previsto dalla normativa, il legislatore, in linea con quello comunitario, ha stabilito poi una serie di regole sia processuali sia sostanziali a favore dell'interessato, nonché norme volte a tutelarlo dai possibili danni conseguenti un illecito trattamento dei dati.

Fra queste occupa un ruolo importante l'art. 15 del Codice, il quale prevede che: "1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo

[180] Provvedimento del 28 maggio 1997, in www.garanteprivacy.it

[181] Art. 12. Codici di deontologia e di buona condotta

1. Il Garante promuove nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, ne verifica la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto.

2. I codici sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana a cura del Garante e, con decreto del Ministro della giustizia, sono riportati nell'allegato A) del presente codice.

3. Il rispetto delle disposizioni contenute nei codici di cui al comma 1 costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici.

4. Le disposizioni del presente articolo si applicano anche al codice di deontologia per i trattamenti di dati per finalità giornalistiche promosso dal Garante nei modi di cui al comma 1 e all'articolo 139.

VEDI G. RASI, *Progresso tecnologico e sviluppo civile*, op. cit; G. SANTANIELLO, *I codici di deontologia nel trattamento dei dati personali*, in www.interlex.it del 24 ottobre 2002

2050 del codice civile. 2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

La terminologia utilizzata sembra ricomprendere tutti i danni derivabili da qualunque operazione di trattamento, inoltre, il rinvio operato all'art. 2050 del c.c. induce a considerare il trattamento dei dati quale attività pericolosa e, quindi, soggetta alla relativa disciplina.[182]

Si segnalano, infine, le recenti modifiche al T.U. della privacy, attraverso le quali in particolare si è proceduto ad un inasprimento delle sanzioni amministrative ed all'estensione dell'area degli illeciti penali[183].

4. Il percorso europeo[184]

Il percorso europeo che ha portato a riconoscere la protezione dei dati personali come diritto fondamentale della persona è iniziato con la stipula nel 1950 della Convenzione per la salvaguardia dei diritti umani e delle libertà fondamentali.

---

[182] S.NIGER, *Le nuove dimensioni della privacy*, op. cit.; alcuni autori, invece, propendono per un'interpretazione del rinvio (prima operato dall'art 18 della l. 675/96) finalizzato esclusivamente all'inversione dell'onere della prova, senza ritenere di inquadrare il trattamento dei dati fra le attività pericolose, vedi ad esempio M. FRANZONI, *dati personali e responsabilità civile*, in Responsabilità civile e previdenza, 1998; P. ZIVIZ, *Trattamento dei dati personali e responsabilità civile: il regime previsto dalla legge 675*, in Responsabilità civile e previdenza, 1997; G. COMANDé, *Commento all'art. 18*, in C.M. BRANCA , F.D. BUSNELLI (a cura di), Tutela della privacy, in Le nuove leggi commentate, 1999.

[183] Modifiche introdotte dalla legge 27 febbraio 2009, n. 14 di conversione, con modificazioni, del decreto-legge n. 207 del 30 dicembre 2008 e dal d.lg. 30 maggio 2008, n. 109, di attuazione della direttiva 2006/24/Ce riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione

[184] Per quanto riguarda, invece, i numerosi documenti internazionali, si segnalano fra gli altri: in ambito OCSE, le Linee-guida sulla protezione della privacy e il flusso transfrontaliero di dati personali, adottate dal Consiglio dell'OCSE il 23 settembre 1980, seguite dalla Dichiarazione sui flussi transfrontalieri di dati, adottata dai Governi dei Paesi membri dell'OCSE l'11 aprile 1985, dalla Dichiarazione ministeriale sulla protezione della privacy sulle Reti globali del 1998 e Linee guida sulla sicurezza dei sistemi e delle reti d'informazioni del 2002, consultabili su http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00&&enUSS_01DBC.html.

La Dichiarazione dei Principi, firmata da 191 paesi in occasione del Il Vertice Mondiale sulla Società della Informazione (WSIS) Ginevra 2003, organizzato dalle Nazioni Unite, consultabile su http://www.quadernionline.it/wsis_2005/_CACCIAGUERRA_RANGHIERI.html; Dichiarazione di Montreux, "La protezione dei dati personali e della privacy in un mondo globalizzato:un diritto universale che rispetta le diversità"; 27ma Conferenza Internazionale delle Autorità di protezione dei dati e della privacy, Montreux, 14-16 settembre 2005, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1170512.

In ambito extraeuropeo, i Ministri della Cooperazione EconomicaAsia-Pacifico (APEC) hanno adottato nel novembre 2004 l'APEC Privacy Framework, successivamente modificato nel 2007, con l'istituzione, fra l'altro, dell' APEC Cross-border Privacy Enforcement Arrangement (CPEA), avente le funzioni di coordinamento, informazione e promozione della normativa sulla privacy fra le autorità dei paese aderenti all'Apec. Vedi http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce/cpea.html.

L'art 8 della CEDU, che trae origine dall'art 12 della Dichiarazione Universale dei diritti dell'uomo del 10 dicembre 1948[185], ha previsto le prime disposizioni volte alla tutela della vita privata a familiare. Tuttavia, è soprattutto attraverso l'interpretazione fattane dalla Corte europea dei diritti dell'uomo che si è venuto a determinare e progressivamente ad ampliare il significato da ascrivere ai concetti di "vita privata"[186] e "corrispondenza"[187], gettando le basi per la positivizzazione del diritto al controllo consapevole su ogni forma di circolazione delle proprie informazioni personali.

Inoltre, l'interpretazione della CEDU - nel caso specifico, dell'art. 8 - ha ad opera della Corte riconosciuto a tale norma un'efficacia orizzontale, oltre che verticale, nel senso che essa si applica anche alle violazioni commesse dai soggetti privati nei confronti di altri individui e non solo dagli Stati membri[188].

Sempre nell'ambito del Consiglio d'Europa, il trattamento dei dati personali è stato poi oggetto di altri atti: si tratta della Convenzione del 28 gennaio 1981 sul trattamento dei dati personali[189], con successivo

[185] Art 12 Dichiarazione Universale dei diritti dell'uomo: "Nessuno sarà oggetto di ingerenze arbitrarie nella sua vita privata, nella sua famiglia, nel suo domicilio o nella sua corrispondenza, né di lesioni al suo onore ed alla sua reputazione. Ogni persona ha diritto alla protezione della legge contro simili ingerenze e lesioni." Consultabile su http://www.privacy.it/diruomo.html. Si veda anche art. 17 del Patto internazionale sui diritti civili e politici del 1966: "1. Nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua famiglia, nella sua casa o nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione. 2. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze od offese." Consultabile su http://www.studiperlapace.it/documentazione/patti.html#p2

[186] Alla tutela della vita privata la Corte ha ricondotto il diritto di mantenere i legami personali (CEDU C. c. Belgio 7.8.1996), il diritto al nome (CEDU Burghartz vedi Svizzera 22.2. 1994, CEDU Stjerna c. Finlandia 25.11. 1994), il diritto alla protezione dei dati personali che attengono alla vita privata (Comm.eur.dir. uomo Leander c. Svezia 17.5.1985) o meno (CEDU Rotaru vedi Romania 4.5.2000), il diritto ad avere informazioni circa l'ambiente (CEDU Guerra ed altri c. Italia 19.2.1998, CEDU McGinnis e Egan c. Regno Unito 9.6.1998), il diritto di mantenere uno stile di vita in quanto appartente ad un gruppo minoritario (Comm.eur.dir.uomo G. e E. c. Norvegia 3.10.1983). Ancora, il 27 luglio 2004, con la sentenza del caso Sidabras vs. Lithuania (Corte Europea dei Diritti Umani, Seconda sezione, Caso Sidabras and Džiautas vs. Lithuania, istanze n. 55480/00 e 59330/00), la Corte Europea dei Diritti dell'Uomo ha dato un'interpretazione molto estensiva del diritto alla privacy previsto dall'art. 8 della Convenzione europea dei diritti dell'uomo. Ha ritenuto, infatti, che la tutela prevista da questo articolo si estenda fino a comprendere il diritto di ciascuno a sviluppare relazioni sociali al riparo da ogni forma di discriminazione o stigmatizzazione sociale, così consentendogli anche il pieno godimento della sua vita privata. La Corte ha dunque considerato la complessiva collocazione della persona nella società, affermando che il pieno rispetto della privacy è una condizione per l'eguaglianza e il godimento di diritti fondamentali, come quello al lavoro.

[187] CEDU, Sentenza Malone c.Regno Unito, 2 agosto 1984 (corte plenaria) serie A n.82; Sentenza Gaskin c. Regno Unito, 7 luglio 1989, corte plenaria, serie A n.160; Sentenza Z. c. Finlandia, 25 febbraio 1997.

[188] Corte europea, 26 marzo 1985, X et Y c. Paesi Bassi, seria A n 91 in Raccolta p11, consultabile anche in B. MICOLANO, *Il diritto antidiscriminatorio nella giurisprudenza della Corte Europea dei diritti dell'uomo*, Giuffrè,Milano, 2009, pag 277.

[189] Ratificata in Italia con legge 21 febbraio 1989 n 98. Consultabile su http://www.privacy.it/convstrasb.html.

Protocollo addizionale dell'8 novembre 2001, a cui si sono aggiunte numerose Raccomandazioni del Comitato dei Ministri[190].

In particolare con la suddetta Convenzione è stato individuato un nucleo di principi relativi al trattamento dei dati personali che si è progressivamente sviluppato negli atti successivi sia del Consiglio d'Europa sia dell'Unione europea[191].

La Convenzione contiene, infatti alcune linee fondamentali, quali: l'attribuzione ai singoli Stati membri della scelta di estendere a meno la tutela ai dati riferiti ad entità giuridiche; la liceità del trattamento dei dati sensibili solo a condizione che gli Stati membri adottino idonee garanzie; l'attribuzione alle persone interessate dei diritti di accesso ai loro dati, di rettifica, di cancellazione.

Si tenga, inoltre, presente che, a differenza delle altre Convenzioni, questa è aperta a qualsiasi altro Stato, anche non membro del Consiglio d'Europa, dietro invito di adesione del Comitato dei Ministri.

A sancire lo stretto legame fra la protezione dei dati personali e il diritto alla vita privata e, dunque, fra l'art 8 della CEDU e la citata Convenzione è stata appunto la Corte di Strasburgo, per la quale la protezione dei dati personali costituisce un'"applicazione settoriale" del diritto al rispetto della vita privata, considerando il "ruolo fondamentale che gioca la protezione dei dati a carattere personale per l'esercizio della vita privata"[192].

In particolare, la Corte ha affermato che la memorizzazione e/o la comunicazione di dati a carattere personale costituisce un'ingerenza nel rispetto della vita privata[193] e ha pertanto stabilito - in maniera estensiva – che anche la raccolta di dati di natura pubblica può rilevare per il rispetto della vita privata, allorché siano raccolti e memorizzati in maniera sistematica in banche dati e registri tenuti dalla autorità pubbliche.

---

[190] La consultazione delle Raccomandazioni del Comitato dei Ministri del Consiglio d'Europa (composto dai Ministri degli Esteri dell'Unione Europea), è importante per comprendere gli standard di correttezza richiesti nei singoli settori. In alcuni casi il Codice della privacy fa ad essi un richiamo espresso: es. art. 61.1 vincola nell'elaborazione del contenuto del codice di deontologia sull'uso di dati pubblici a tenere presente quanto previsto dalla Raccomandazione R(91) 10 del Consiglio d'Europa. L'elenco delle Raccomandazioni è consultabile all'interno del sito www.garanteprivacy.it.

[191] M. SGROI (a cura di), *Nuovi ambiti di tutela della personalità* op cit.; M. MIGLIAZZA, *Profili internazionali ed europei del diritto all'informazione e alla riservatezza*. Giuffè, Milano, 2004.

[192] Sentenza 25 febbraio 1997, Z v Finlandia, Raccolta delle sentenze e decisioni, 1997-I.

[193] Sentenza 26 marzo 1987, Leander vedi Svezia serie A n. 116, ; sentenza 16 febbraio 2000 Amman v. Svizzera, in Eur. Court HR, II, 2000, p. 2031 e raccolta delle sentenze e decisioni 2000-II, par. 65.

Sullo Stato incombe, quindi, secondo la Corte sia un obbligo negativo, nel senso che i dati non devono essere indebitamente divulgati contro la volontà del soggetto interessato, sia un obbligo positivo volto a permettere l'accesso dello stesso soggetto ai propri dati personali, eventualmente raccolti dalla pubblica autorità[194].

In ogni caso, la Corte ha affermato costantemente che l'assenza di una base legale per la raccolta e la diffusione di dati personali, così come la sussistenza di una legge che non sia tuttavia accessibile alla persona interessata e prevedibile per quanto riguarda i suoi effetti, costituisce una violazione dell'art. 8 CEDU[195].

Quanto alla Comunità europea, invece, questa si è occupata direttamente della materia solo diverso tempo dopo.

E', infatti, con la Direttiva del Parlamento europeo e del Consiglio n. 95/46/CE[196] che, riprendendo i principi della suddetta Convenzione, la Comunità europea finalmente ha introdotto un più completo sistema di garanzia dei dati personali.

Obiettivo di tale Direttiva, come di altre nel settore, è invero quello di contemperare la tutela delle libertà delle persone – in particolare in relazione al trattamento dei dati personali – con l'esigenza della libera circolazione dei dati fra gli Stati membri, funzionale a sua volta all'esercizio delle libertà di circolazione delle persone, beni e servizi e, quindi, al buon funzionamento del mercato unico, scopo questo per cui è stata inizialmente costituita la Comunità europea[197].

---

[194] Sentenza Leander cit; sentenza 7 luglio 1989, Gaskin v. Regno Unito, serie A n. 160; Malone c. Regno Unito, 2 agosto 1984 serie A n. 82.

[195] Cfr. Sentenza 4 maggio 2000, Rotaru v. Romania, in Raccolta delle sentenze e delle decisioni 2000-V, par. 43; sentenza Leander cit, sentenza Amman cit., sentenza 28 ottobre 1994, Murray v. Regno Unito, serie A n. 300-A, sentenza 29 giugno 2006, Panteleyenco v. Ucraina, ricorso11901/02, Raccolta delle sentenze e decisioni 2006 ; Sentenza del 19 febbraio 1998 Ricorso n° 14967/8, Guerra ed altri c. Italia, consultabile su http://www.dirittiuomo.it/ Corte%20-Europea/Italia/ 2002/Guerra.htm.

[196] In GUCE L 282/31 del 23 novembre 1995, consultabile su http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Normativa%2FComunitaria+e+internazionale%2FUnione+europea.

[197] Cfr. F. PIZZETTI, *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, in P. BILANCIA e M. D'AMICO (a cura di) La nuova Europa dopo il Trattato di Lisbona, Giuffrè, Milano, 2009; G. TIBERI, *Riservatezza e protezione dei dati personali*, op. cit., pag 378; U. PAGALLO, *La tutela della Privacy negli Stati Uniti D'America e in Europa*, op. cit., pag.116. A fondamento di tale interpretazione viene richiamato, tra l'altro, il fatto che l'ambito di applicazione della disciplina sulla protezione dei dati sia circoscritto, ai sensi dell'art. 3, par. 2, 1° trattino della direttiva, ai soli trattamenti svolti nell'ambito di attività rientranti nel campo di applicazione del diritto comunitario. Vedi in questo senso R. PARDOLESI., *Dalla riservatezza alla protezione dei dati personali*, in R. PARDOLESI (a cura di), Diritto alla riservatezza e circolazione dei dati personali, Giuffrè, Milano, 2003, p. 36. Come evidenziato nel seguito della trattazione, la Corte di Giustizia delle Comunità Europee, tuttavia, ha interpretato in modo restrittivo tale limitazione, ritenendo che un'attività non risulta estranea alla sfera del diritto

Tuttavia, fin dagli anni settanta, la Corte di giustizia è venuta sempre più riconoscendo la necessità d'inserire i diritti umani nel sistema giuridico comunitario, pensato originariamente, come detto, soprattutto in chiave di integrazione economica.

Per giustificare la tutela dei diritti non espressamente riconosciuti nella disciplina comunitaria, la Corte ha utilizzato il criterio ermeneutico dei "principi generali del diritto".

A partire dalle cause Internationale Handelsgesellschaft del 1970[198], Nold del 1974[199] e Hauer del 1979[200] la Corte, infatti, ha sostenuto che la tutela dei diritti umani costituisce "parte integrante" del diritto comunitario, richiamandosi alle tradizioni costituzionali comuni degli Stati membri[201] e, in parte, alla Convenzione europea dei diritti dell'uomo[202].

comunitario per il solo fatto di non avere un legame diretto con l'esercizio delle libertà fondamentali garantite dal Trattato.

198 Sentenza C-11/70, Internationale Handelsgesellschaft MBH – Einfuhr - und vorratsstelle fuer getreide und futtermittel, del 17 dicembre 1970, in Racc. 1970, p. 1125, consultabile su http://www.giurcost.org/casi_scelti/CJCE/C-11-70.htm: "3 Il richiamo a norme o nozioni di diritto nazionale nel valutare la legittimità di atti emananti dalle istituzioni della Comunità menomerebbe l' unità e l' efficacia del diritto comunitario. La validità di detti atti può essere stabilita unicamente alla luce del diritto comunitario. Il diritto nato dal Trattato, che ha una fonte autonoma, per sua natura non può infatti trovare un limite in qualsivoglia norma di diritto nazionale senza perdere il proprio carattere comunitario e senza che sia posto in discussione il fondamento giuridico della stessa Comunità.

Di conseguenza, il fatto che siano menomati vuoi i diritti fondamentali sanciti dalla Costituzione di uno Stato membro, vuoi i principi di una costituzione nazionale, non può sminuire la validità di un atto della Comunità nè la sua efficacia nel territorio dello stesso Stato.

4 E' tuttavia opportuno accertare se non sia stata violata alcuna garanzia analoga, inerente al diritto comunitario. La tutela dei diritti fondamentali costituisce infatti parte integrante dei principi giuridici generali di cui la Corte di giustizia garantisce l' osservanza. La salvaguardia di questi diritti, pur essendo informata alle tradizioni costituzionali comuni agli Stati membri, va garantita entro l' ambito della struttura e delle finalità della Comunità.

Si deve quindi accertare, alla luce dei dubbi manifestati dal giudice proponente, se la disciplina delle cauzioni abbia leso dei diritti fondamentali la cui osservanza va garantita nell' ordinamento giuridico comunitario."

199 Sentenza causa 4/73, del 14 maggio del 1974, J. Nold, Kohlen- und Baustoffgrosshandl contro Commissione delle Comunità europee, in Racc., 1974, pag. 491, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= CELEX:61973J0004:IT:HTML. In riferimento ai Trattati internazionali relativi alla tutela dei diritti dell'uomo:"la Corte, garantendo la tutela di tali diritti, è tenuta ad ispirarsi alle tradizioni costituzionali comuni agli Stati membri e non potrebbe, quindi, ammettere provvedimenti incompatibili con i diritti riconosciuti e garantiti dalle Costituzioni di tali Stati . I trattati internazionali relativi alla tutela dei diritti dell'uomo cui gli Stati membri hanno cooperato o aderito possono del pari fornire elementi di cui occorre tener conto nell'ambito del diritto comunitario".

200 §§12-16, sentenza, causa 44/79, 13 dicembre 1979, Hauer contro Land Rheinland-Pfalz, in Racc 1979 pagina 3727, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:61979J0044:IT:HTML, http://www.giurcost.org/casi_scelti/CJCE/C-44-79.htm.

201 Tra i tanti vedi L. COZZOLINO, *Le tradizioni costituzionali comuni nella giurisprudenza della Corte di giustizia delle Comunità europee*, consultabile su http://www.associazionedeicostituzionalisti.it/materiali/convegni/copanello020531/ cozzolino.html.

202VEDI § 32 Sentenza, causa 36/75, del 28 ottobre 1975, Roland Rutili Contro Ministro dell'Interno - (Domanda di pronunizia pregiudiziale, proposta dal Tribunale Amministrativo di Parigi), Racc. 1975, pag. 1219, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:61975J0036:IT:HTML. Vedi tra i tanti, G.M. DE MURO, I rapporti fra Corte di giustizia delle comunità europee e Corte europea dei diritti dell'uomo, consultabile su

Ancora, nella sentenza Panasonic del 1979[203], la Corte ha affermato che la protezione dei dati personali è prevista dall'ordinamento comunitario come uno degli aspetti impliciti nel più ampio diritto del soggetto al rispetto della sua vita privata.

Sempre in ambito di protezioni dei dati personali, significative sono due sentenze, entrambe del 2003, in cui i giudici hanno deciso per l'applicabilità della Direttiva n. 95/46, nonostante le questioni che si trovavano a decidere non presentassero un collegamento diretto con il diritto comunitario[204].

In tal modo ben prima dell'adozione di testi normativi che hanno previsto puntualmente il riconoscimento dei diritti umani e, in particolare, della privacy come diritto garantito all'interno del sistema giuridico comunitario, quest'ultimo li ha tutelati soprattutto per via giurisprudenziale.

In ogni caso, un merito della Direttiva va sicuramente individuato nell'aver saputo "abbracciare" le molte facce del rapporto fra l'evoluzione tecnologica e la gestione delle informazioni, mediante la creazione di un sistema di principi, ruoli e responsabilità che alla prova dei fatti si è dimostrato piuttosto solido, in grado di vincolare gli Stati membri a

---

http://www.associazionedeicostituzionalisti.it/materiali/convegni/copanello020531/demuro.html; G. TIBERI, Riservatezza e protezione dei dati personali, op. cit.

[203] §§ 18 e 19, sentenza, causa 136/79, 26 giugno 1980del 1979, National Panasonic v. Commissione, in Racc., 1980, p. 2033.

[204] Sentenza 6 novembre 2003 (causa C 101/01), Lindqvist, G.U.U.E n. C 007 del 10/01/2004 pag. 0003 – 0004; vedi anche Foro it., 2004, IV, 57; consultabile anche su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:007:0003:0004:IT:PDF e su http://assemblealegislativa.regione.emilia-romagna.it/biblioteca/pubblicazioni/MonitorEuropa/2003/Monitor18/Corte_Giustizia/Causa_101_01_ Internet.doc. Qui la Corte ha ritenuto che la clausola relativa alle attività "non rientranti nel campo di applicazione del diritto comunitario" si riferisce alle sole attività proprie degli Stati o delle autorità statali ed estranee ai settori di attività dei singoli, alle quali non risultavano quindi equiparabili le attività a carattere religioso, svolte a titolo di volontariato nell'ambito della Parrocchia, esercitate nel caso di specie dalla sig.ra Lindqvist (§§ 43, 45 e 48 della sentenza, visionabile anche su in http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=IT&numdoc=62001J0101&model=guichett). La Corte ha così respinto l'opinione, sostenuta dall'Avvocato Tizzano nelle sue conclusioni generali presentate il 19 settembre 2002, secondo la quale il trattamento in causa non poteva dirsi effettuato per l'esercizio di attività rientranti nel campo di applicazione del diritto comunitario, bensì di attività a carattere non economico prive di qualsiasi legame con l'esercizio delle libertà fondamentali garantite dal Trattato, condotte a titolo gratuito e al di fuori di qualsiasi rapporto lavorativo, in seno alla comunità parrocchiale (§§ 35 e 36 del parere, in http://www.infogiur.com/giurisprudenza/privacy_corteUE_6_11_03_conclusioni.asp). Su tali aspetti vedi A. CALMIERI, R PARDOLESI., *Il codice in materia di protezione dei dati personali e l'intangibilità della "privacy" comunitaria*, in Il Foro It., 2004, IV, pp. 57- 64, consultabile anche su http://www.law-economics.net/public/Palmieri %20e%20Pardolesi%20sul%20caso% 20Lindqvist.pdf.

Sentenza 20 Maggio 2003 (Cause riunite C-465/00, C-138/01 e C-139/01) Rechnungshof , GUUE del 19 luglio 2003, C 171/3 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2003:171:0003:0004:IT:PDF); consultabile su http://www.lex.unict.it/eurolabor/documentazione/sentenze/causa139-01.htm. Vedi anche G. GARBI, *L'importanza delle sentenze della Corte Europea di Giustizia nel processo di giuridificazione dei diritti della persona ed in particolare della privacy*, in Diritto e diritti - Rivista giuridica elettronica pubblicata su Internet, consultabile su www.diritto.it/archivio/1/20682.pdf; G.TIBERI, *Riservatezza e protezione dei dati personali*, op. cit., pag 379.

conformarsi ad esso, lasciando, comunque, agli stessi significativi margini di adattamento.

Particolarmente rilevanti per la longevità dell'impianto previsto dalla Direttiva sono: l'apertura delle nozioni di trattamento e di dato personale, l'ampiezza dei diritti dell'interessato, la spinta a creare, nei singoli Stati membri, Autorità garanti a presidio della materia e l'istituzione di un Gruppo di lavoro comunitario di raccordo fra le Autorità garanti nazionali, il cd. *Working Party*, che si è rivelato molto importante nell'opera di interpretazione delle norme esistenti e nel contributo offerto alla successiva evoluzione normativa[205].

Quindi, sebbene finalizzata a quelli che erano gli obiettivi della Comunità, ovvero l'introduzione di un mercato unico, fin dal suo nascere la disciplina comunitaria della privacy, soprattutto nel suo aspetto dinamico di tutela del trattamento dei dati personali, si è posta un obiettivo di alto profilo: la tutela della persona e della sua dignità nella cornice delle libertà fondamentali[206].

Va poi precisato che il contesto di riferimento della Direttiva era, comunque, la tutela dei dati personali nell'ambito del cd. Primo Pilastro dell'Unione[207]

Sempre dello stesso periodo, si segnala la Direttiva del Parlamento e del Consiglio 97/66 CE del 15 dicembre 1997[208], sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, che ha disciplinato in modo specifico la relazione fra i servizi di telecomunicazioni su rete pubbliche e la tutela della privacy, in seguito allo sviluppo della società dell'informazione.

---

[205] Il Gruppo Europeo dei Garanti, cd Working Party è stato istituito dall'art 29 della direttiva n. 95/46/CE. Il lavori del Gruppo sono consultabili su www.europa.eu.int/comm/internal_market/privacy/workinggroup_en.htm; il Gruppo dei Garanti Europeo è stato presieduto dal 2000 al 2004 dal Prof. Stefano RODOTà, ex presidente dell'Autorità Italiana.

[206] Cosi M. SGROI(a cura di), *Nuovi ambiti di tutela della personalità*, op cit., pag 196; vedi anche S. RODOTà, *Tra diritti fondamentali ed elasticità della normativa:il nuovo Codice della privacy*, in Europa *e* diritto privato, 2004, fasc. 1, pp. 1-10.

[207] I cd. tre pilastri dell'Unione europea, posti con il Trattato di Maastricht del 1992, hanno suddiviso le politiche dell'Unione europea in tre aree fondamentali. Il primo riguarda le Comunità europee, il secondo la Politica estera e di sicurezza comune, il terzo la Cooperazione giudiziaria e di polizia in materia penale.

[208] In GUCE L24/l del 30 gennaio 1998, consultabile su http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Normativa%2FComunitaria+e+internazionale%2FUnione+europea.

Nel caso in cui il rapporto riguardi le persone fisiche direttamente nei confronti delle istituzioni e degli organismi comunitari, viene in rilievo il Regolamento n 45/2001 del 18 dicembre 2000[209] .

Il Regolamento ha come riferimenti le Direttive 95/46 e 97/66, poiché è necessario "garantire in tutto il territorio nazionale un'applicazione coerente ed omogenea della norme relative alla tutela delle libertà e dei diritti fondamentali delle persone fisiche con riguardo al trattamento dei dati personali", al fine anche di assicurare la libera circolazione dei dati personali fra le istituzioni comunitarie e gli Stati membri e fra le istituzioni comunitarie e gli organismi comunitari stessi[210].

Viene, inoltre, istituita un'autorità di controllo indipendente, il Garante europeo per la protezione dei dati, la cui attività è disciplinata dal regolamento, con funzioni di vigilanza sull'esatta applicazione delle norme contenute nel Regolamento n. 45/2001 da parte delle istituzioni ed organismi comunitari[211].

Lo sviluppo delle tecnologie e in particolare dei sistemi di comunicazione elettronica ha portato, successivamente, all'approvazione della Direttiva n. 2002/58 CE[212] (anche detta direttiva "e-privacy) che ha sostituito la precedente Direttiva n. 97/66 sulle telecomunicazioni, al fine di garantire un'adeguata tutela del diritto alla protezione dei dati personali per le persone fisiche e la tutela dei legittimi interessi degli abbonati che siano anche persone giuridiche.

Proprio nell'ottica di creare un sistema di garanzie e di tutele nel mondo delle comunicazioni elettroniche sono seguite, poi, altre direttive, fra cui la Direttiva n. 2006/24 Ce, "riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura dei servizi di comunicazione elettronica accessibili al pubblico e di reti pubbliche di comunicazione"[213] e la Direttiva

[209] In GUCE L 8 /l del 12 gennaio 2001, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0045:IT:HTML.

[210] Dodicesimo considerando del regolamento 45/2001.

[211] V art. 1.2 e, in particolare, artt. 41-48 del regolamento 45/2001 che disciplinano le funzioni, le competenze la nomina da parte del Parlamento europeo e del Consiglio di comune accordo per cinque anni.

[212] GUCE n. L 201 del 31/07/2002, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=35284.

[213] GUCE n. l. 105/54 del 13 /4/2006, consultabile su http://www.garanteprivacy.it/garante/document?ID=1485189.

n. 2009/136/CE[214]. Entrambe hanno modificato la precedente Direttiva del 2002.

In particolare, la Direttiva n. 2006/24 Ce, nota anche come Direttiva "data retention" è stata adottata per tenere conto sia delle innovazioni tecnologiche, nel frattempo intercorse, sia per introdurre disposizioni specificatamente volte ad innalzare, nel quadro della lotta al terrorismo, il livello e le modalità di trattamento e di conservazione dei dati prodotti nell'ambito delle comunicazioni elettroniche, suscitando in tal senso non poche polemiche[215].

La stessa ha imposto, infatti, ad operatori e providers di tutta Europa, dopo il recepimento dei vari governi[216], la registrazione da uno a tre anni dei log degli accessi ad Internet, dei mittenti e dei destinatari delle e-mail o delle telefonate e della localizzazione di chi chiama da un cellulare.

Quanto al riconoscimento generale della privacy come diritto, si è già evidenziato che nel 2000 è stata approvata la Carta dei diritti fondamentali dell'Unione europea[217], frutto di una lenta ma incessante conquista della tutela dei diritti fondamentali da parte dell'ordinamento comunitario.

---

[214] Direttiva del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori Testo rilevante ai fini del SEE. GUCE n. L 337 del 18/12/2009, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009: 337:0011:01:IT:HTML.

[215] Si veda il parere del Gruppo di lavoro europeo (Working Party), Parere 3/2006 consultabile su http://ec.europa.eu/ justice_home /fsj / privacy/docs/wpdocs/2006/wp119_it.pdf, in cui si legge, tra l'altro "Il gruppo di lavoro articolo 29 osserva che nella direttiva mancano alcune adeguate e specifiche salvaguardie riguardo al trattamento dei dati comunicati e che vi è lasciato spazio per un'interpretazione e attuazione divergenti tra gli Stati membri. È invece necessario prevedere salvaguardie adeguate e specifiche per tutelare gli interessi vitali degli individui, quali sono menzionati nella direttiva 2002/58/CE, in particolare il diritto alla riservatezza quando si utilizzano servizi pubblici di comunicazione elettronica. Inoltre, il gruppo di lavoro ritiene d'importanza cruciale che le disposizioni della direttiva siano interpretate e attuate secondo modalità armonizzate, così da assicurare ai cittadini il medesimo grado di tutela in tutta l'Unione europea.".

In conseguenza della suddetta direttiva, con la Decisione 2008/324/CE, GUUE l111 del 23/4/2008, consultabile su http://www.eliss.org/new/eu/2008_324_CE.pdf , la Commissione ha stato istituito il gruppo di esperti «Piattaforma per la conservazione di dati elettronici a fini d'indagine, accertamento e perseguimento di reati gravi».

Ancora per una riforma della Direttiva 2006/24 si veda L. BOLOGNINI e P. PAGANINI, *La libertà di Internet e reati: sì all'anonimato protetto,* consultabile su http://mediablog.corriere.it/2009/12/liberta_di_internet_e_reati_si.html.

[216] In Italia è stata adottata con D.lgs. del 30 maggio 2008, n 109, consultabile su http://www.governo.it/Governo/ Provvedimenti/dettaglio.asp?d=39107.

[217] Carta dei diritti fondamentali dell'Unione europea, proclamata nuovamente in una versione riveduta nel 2007 a Strasburgo, GUCE n C 303/1, 14 dicembre 2007, consultabile su http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do?uri=OJ:C:2007:303:0001:0016:IT:PDF.

Risultato per il quale, si è visto, anche la giurisprudenza della Corte di giustizia ha avuto un ruolo fondamentale.

Il documento di Nizza, nonostante non sia stato esente da critiche, soprattutto per quanto riguarda il riconoscimento dei diritti sociali, ha posto la persona al centro di ogni azione comunitaria. La Carta ha riaffermato "principi comuni a vari Stati nazionali, formulati dalla giurisprudenza della Corte di Giustizia o tratti dalle tradizioni costituzionali e il testo parla a tutti offrendo una sintesi ed un orientamento per i giuristi impegnati in attività pratiche e teoriche"[218].

Per quanto riguarda in particolare la privacy, la Carta ha operato una distinzione tra il tradizionale diritto al rispetto della propria vita privata e familiare (art. 7) e il diritto alla protezione dei dati personali (art. 8), che si configura così come un diritto fondamentale nuovo e autonomo.

" La distinzione" – operata dalla Carta – " non è di facciata. Nel diritto al rispetto alla vita privata e familiare si manifesta soprattutto il momento individualistico, il potere si esaurisce sostanzialmente nell'escludere interferenze altrui: la tutela è statica, negativa. La protezione dei dati, invece, fissa regole sulle modalità del trattamento dei dati, si concretizza in poteri di intervento: la tutela è dinamica, segue i dati nella loro circolazione.

I poteri di controllo e di intervento, inoltre non sono attribuiti soltanto ai diretti interessati, ma vengono affidati anche ad una Autorità indipendente (art. 8.3) (…).

Si evidenzia bene qui il punto d'arrivo di una lunga evoluzione del concetto di privacy, dall'originaria sua definizione come diritto ad essere lasciati soli fino al diritto a mantenere il controllo delle proprie informazioni e di determinare le modalità della costruzione della propria sfera privata"[219].

Come noto, la Carta è stata inserita successivamente nel Trattato che adotta una Costituzione per l'Europa, firmato a Roma il 24 ottobre 2004, ma mai entrato in vigore a causa della stop imposto alla ratifiche dai referendum negativi di Francia e Olanda.

[218] G. VETTORI, *Carta europea e diritti dei privati*, Cedam, Padova, 2002. S. RODOTà osserva che la Carta "sposta l'attenzione dalla sola logica economica a quella dei diritti , e dunque dalle imprese ai cittadini; si presenta come il nucleo du una futura, e compiuta costituzione europea", in *Libertà personale .Vecchi e nuovi nemici*, in BOVERO. (a cura di), Quale libertà. Dizionario minimo contro i falsi liberali,op. cit..

[219] S. RODOTà, *Tra diritti fondamentali ed elasticità della normativa,* op cit. pag 3.

Molte delle innovazioni della Costituzione sono state però incluse nel successivo Trattato di Lisbona[220], entrato in vigore, anche esso con non poche difficoltà, il 1º dicembre 2009.

La Carta non è più contenuta nel Trattato, ma ha acquistato, ai sensi dell'art. 6 del Trattato sull'Unione europea, come modificato dal Trattato di Lisbona, lo stesso valore giuridico dei Trattati[221].

Negli ultimi anni, inoltre, il bisogno di sicurezza legato alla minaccia terroristica ha condotto l'Unione Europea ad un rafforzamento delle modalità di collaborazione tra le strutture di sicurezza e di contrasto alla criminalità, con la conseguente estensione della raccolta, conservazione ed elaborazione dei dati personali ai fini di sicurezza, di polizia e di giustizia. Tutto questo ha reso sempre più pressante la necessità di predisporre ulteriori e specifici strumenti di protezione dei dati personali, al fine di garantire un livello di protezione più elevato.

In questo solco, con il Trattato di Lisbona, il processo di estensione dei principi sulla protezione dei dati ha compiuto significativi passi avanti: da un lato, infatti, nell'ambito dell'unificazione dei Pilastri, il Trattato stabilisce che la protezione dei dati personali deve trovare adeguata collocazione e disciplina anche nei settori della sicurezza interna ed esterna, dall'altro è

---

[220] http://europa.eu/lisbon_treaty/index_it.htm; Cfr M. E. GENNUSA, *Dal Trattato Costituzionale al Trattato di Lisbona (27 febbraio 2008)*, consultabile http://economia.unipv.it/pagp/pagine_personali/gennel/materiale/ Dal%20Trattato%20costituzionale%20al%20Trattato%20di%20Lisbona.doc; A. PERTICI, *Il Trattato costituzionale nel processo di costituzionalizzazione europea*, consultabile su www.unipi.it/athenet1-14/13/articoli/0013Pertici_boxA.html; P. PASSAGLIA, *Il Trattato che adotta una costituzione per l'Europa. Due anni dopo*, Foro It., 2007, V, 19; J. ZILLER, *Il nuovo Trattato europeo*, Il Mulino,Bologna, 2007; B. NASCIMBENE e A. LANG, *Il Trattato di Lisbona: l'Unione europea a una svolta?*, in Il corriere giuridico, 2007; S. DELLA VALLE, *Una legge fondamentale post-costituzionale? Il diritto pubblico europeo alla luce del Trattato di Lisbona*, consultabile su www.costituzionalismo.it; A. DUFF, *Guida al Trattato di Lisbona*, consultabile su http://www.andrewduffmep.org.uk/resources/sites/217.160.173.25406d96d1812cb6.84417533/EU%20Constitution%20Briefing/Guida+al+trattato+Italiano.pdf; Vedi PAMIO, *Le novità introdotte dal Trattato di Lisbona. Spunti di riflessioni*, consultabile su http://www.giustamm.it/; P. PASSAGLIA, *Il Trattato di Lisbona: qualche passo indietro per andare avanti*, in Il Foro It., 2008, n. 1, pp. 40-44; C. DE FIORES, *Il fallimento della Costituzione europea. Note a margine del Trattato di Lisbona*, in http://www.costituzionalismo.it/ articolo.asp?id=272.

[221] Anche l'art 16 (ex articolo 286 del TCE) del Trattato sul funzionamento dell'Unione europea prevede espressamente il diritto alla protezione dei dati personali e le autorità indipendenti : "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.

Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea. GUUE C 83 del 30 marzo 2010, consultabile su http://eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:IT:PDF.

previsto che, in questi settori, si debbano definire specifiche discipline e regole, così da consolidare il rispetto dei principi già da tempo riconosciuti nell'ambito del Primo Pilastro (art. 39 T.U.E).

Si tratterà, quindi, di adeguare la normativa di protezione dei dati al nuovo quadro politico- istituzionale, tenendo anche in considerazione che una delle novità del Trattato di Lisbona consiste nella "normalizzazione" delle procedure decisionali.

Si avrà, quindi, la tendenziale estensione – conseguente all'unificazione dei Pilastri - degli strumenti normativi a tutti i settori di attività dell'Unione, anche se, come precedentemente osservato, lo stesso Trattato prevede la possibilità di norme specifiche in relazione a determinati settori, tra cui appunto la protezione dei dati personali[222].

Si segnala, infine, la Comunicazione della Commissione del 4 novembre 2010[223], in cui è stato evidenziato che per far fronte alla nuove sfide poste dallo sviluppo delle tecnologia "l'UE deve mettere a punto un approccio generale e coerente onde garantire che il diritto fondamentale di ciascuno alla protezione dei dati personali sia pienamente rispettato all'interno e all'esterno dell'UE". Questo compito deve essere affrontato utilizzando i nuovi strumenti messi a disposizione dal Trattato di Lisbona: "la Carta dei diritti fondamentali dell'Unione europea, il cui articolo 8 riconosce il diritto alla protezione dei dati personali, è divenuta giuridicamente vincolante ed è stata istituita una nuova base giuridica che consente di stabilire norme dell'Unione sistematiche e coerenti di protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e alla libera circolazione di tali dati"[224].

La Commissione, quindi, valuterà in che modo assicurare l'applicazione coerente delle norme di protezione dei dati, tenendo conto delle ripercussioni delle nuove tecnologie sui diritti e sulle libertà delle persone, dell'obiettivo di garantire la libera circolazione dei dati personali nel mercato interno. L'approccio con cui la Commissione svolgerà tale compito

[222] F. PIZZETTI, *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, op. cit..

[223] COM(2010) 609, consultabile su http://www.astrid-online.it/Documenti/Privacy/CE_protezione-dati-personali.pdf

[224] Cfr. l'articolo 16 del trattato sul funzionamento dell'Unione europea (TFUE).

è un approccio globale, perché questa è ormai la dimensione dei problemi da affrontare.

Su tale base, quindi, "a seguito di una valutazione d'impatto e vista la Carta dei diritti fondamentali dell'Unione europea, la Commissione proporrà un atto legislativo nel 2011 per la revisione del quadro giuridico sulla protezione dei dati, con l'intento di consolidare la posizione dell'UE nei confronti della protezione dei dati personali in tutte le politiche europee (…)".

5. Riferimenti di diritto comparato in Europa[225]

5.1. La Spagna

La protezione della privacy in Spagna inizia dalla Costituzione[226], dove all'art 18 è previsto: "1. È garantito il diritto all'onore, all'intimità personale e familiare e alla propria immagine. 2 Il domicilio è inviolabile. Non sarà consentito accedervi o compiervi alcuna perquisizione senza il consenso del titolare o senza una disposizione dell'autorità giudiziaria, salva flagranza di delitto. 3 È garantita la segretezza delle comunicazioni, in particolare postali, telegrafiche e telefoniche, salvo disposizione dell'autorità giudiziaria. 4 La legge limiterà l'uso dell'informatica allo scopo di garantire l'onore e

[225] Per una panoramica generale sulle normative degli altri Stati europei si rinvia al link: Il mondo la privacy in Italia e in Europa su www.privacy.it/linkpriv1.html ed il sito della Commissione europea http://ec.europa.eu/justice/policies/privacy/law/ implementation_en.htm#italy

Per una panoramica generale delle legislazioni degli Stati extraeuropei si rinvia al link: Il mondo la privacy nei Paesi extraeuropei su www.privacy.it/linkpriv2.html.

Ad esempio la Costituzione della Repubblica del Sudafrica, che è del 1993, prevede all'art. 13 intitolato *Privacy*: «Ogni persona avrà diritto alla propria *privacy*; il che includerà il diritto a non essere assoggettato a perquisizioni della propria persona, della casa o della proprietà, a non subire il sequestro di beni privati o la violazione delle proprie comunicazioni private», in P. BISCARETTI di RUFFIA con la collaborazione di M. GANINO, *Costituzioni straniere contemporanee*, vol. II: Le Costituzioni di sette Stati di recente ristrutturazione, a cura di, VI ed. interamente rifatta, Giuffrè, Milano 1996, 25 ss .

Per quanto riguarda l'America Latina, le esperienze sull'*habeas data* costituzionale si possono suddividere tre categorie: *a*) Paesi dove la Costituzione ha previsto in forma diretta, completa e precisa l'*habeas data* (Guatemala, Brasile, Colombia, Paraguay, Perù, Ecuador, Argentina, Venezuela); *b*) Paesi che prevedono la garanzia attraverso la legislazione o in forma indiretta attraverso il ricorso di *amparo costituzionale* (Cile, Costa Rica, Bolivia, Nicaragua, Honduras); *c*) le altre esperienze, che prevedono una tutela indiretta dell'*habeas data* (Panama, Messico, Uruguay e Salvador), cfr. T. E. FROSINI, *Tecnologie e libertà costituzionali*, G. COMANDE' e G. PONZALLI (a cura di) in Scienza e diritto nel prisma del diritto comparato, op. cit., pag 179 e ss., cfr anche T.E. FROSINI, *Libertà informatica:brevi note sull'attualità di una teoria giuridica*, consultabile su http://www.dirittoestoria.it/7/Contributi/Frosini-Libert-informatica.htm#_ftn3.

[226] In ambito europeo, rappresenta, insieme alla Costituzione portoghese (art.35 della Carta del 1976 e artt. 26 e 35 di quella del 1982), la prima espressa costituzionalizzazione del diritto alla riservatezza.

l'intimità personale e familiare dei cittadini ed il pieno esercizio dei loro diritti".

Da un punto di vista sistematico, l'art. 18 è inserito nella Sezione prima (Diritti fondamentali e libertà pubbliche) del Capitolo secondo (Diritti e libertà) del Titolo primo (Diritti e doveri fondamentali) della Costituzione, derivandone peculiarità in ordine alle garanzie legali e alla tutela costituzionale su diversi piani: normativo, istituzionale e giurisdizionale[227].

Dal punto di vista normativo, ad esempio, l'art. 53.1 della Costituzione prescrive che: "I diritti e le libertà riconosciuti nel Capitolo secondo del presente Titolo vincolano tutti i poteri pubblici. Soltanto per legge, che in ogni caso dovrà rispettarne il contenuto essenziale,potrà regolare l'esercizio di tali diritti e libertà [...]". Quanto allo strumento normativo, le leggi che ne regolano l'esercizio devono essere leggi organiche (art. 81 Cost.).

Sempre riguardo all'indicazione costituzionale, decisivo ai fini dell'individuazione dell'ampiezza del contenuto del diritto all'intimità anche in termini dinamici, legati allo sviluppo delle tecnologie, è la relazione tra il I comma dell'art. 18 ed il IV, relativo alla c.d. "libertà informatica", in grado di collegare il diritto alla intimità al il diritto alla "autodeterminazione informativa"[228].

In merito alle determinazione del contenuto del diritto, in virtù della sua costituzionalizzazione, in Spagna questa si deve principalmente all'opera del Tribunal Costitutional[229], che ne ha determinato l'ampiezza e la portata, attraverso una *ponderation de bienes*, quando il diritto alla *intimidad* si è trovato a confliggere con altri diritti di rango costituzionale[230]

---

[227] Vedi G. FAMIGLIETTI, *Il diritto alla riservatezza o la riservatezza come diritto. Appunti in tema di riservatezza ed intimidad sulla scorta della giurisprudenza della Corte costituzionale e del Tribunal Constitucional* . op cit

[228] Il Tribunale costituzionale ha fatto per la prima volta riferimento al concetto di autodeterminazione informativa nella sentenza n. 292 del 30 novembre del 2000, sulla scia del Tribunale costituzionale dell Repubblica Federale Tedesca che con la sentenza del 15 dicembre 1983 ha coniato per la prima volta la sudetta espressione. Sentenza consultabile su http://www.tribunalconstitucional.es/es/jurisprudencia/Paginas/Sentencia.aspx?cod=7467; cfr anche J. CUERVO *Autodeterminación Informativa*, consultabile su http://www.informatica-juridica.com/trabajos/autodeterminacion _informativa.asp.

[229] Per una panoramica della principale giurisprudenza costituzionale si veda G. FAMIGLIETTI, *Il diritto alla riservatezza o la riservatezza come diritto. Appunti in tema di riservatezza ed intimidad sulla scorta della giurisprudenza della Corte costituzionale e del Tribunal Constitucional.* op. cit.

[230] Idem., vedi poi ad esempio STC 17 settembre 2001 n. 186/2001; STC 22 aprile 2002, 83/2002, consultabile su http://ocw.usal.es/ciencias-sociales-1/derecho-a-la-informacion/contenidos/SENTENCIAS/1er%20BLOQUE/PDF/STC%20832002.%20de%2022%20de%20abril.pdf; C. SARTORETTI, *Contributo allo studio del diritto alla privacy nell'ordinamento costituzionale. Riflessioni sul modello francese*, Giappichelli, Torino, 2008, pag. 47. Inoltre, si osserva che la pubblica amministrazione spagnola è all'avanguardia mondiale in materia di egovernment (per l'Italia si rinvia al secondo capitolo).

In Spagna sono in vigore dal 14/1/2000, la *Ley Orgánica n.15 de Protección de Datos de Carácter Personal* (LOPD) del 13 dicembre 1999, con la quale è stata data attuazione anche in Spagna alla Direttiva europea del 25 ottobre 1996 (95/46/CE), e il *Regolamento n. 994/1999* sulle misure minime di sicurezza[231].

L'irruzione delle nuove tecnologie ha determinato successivamente l'emersione di una nuova specie di dati, in origine estranei alla nozione ordinaria di dato personale: si tratta dei dati sul traffico e dei dati di localizzazione. Per questo motivo il legislatore ha adottato due ulteriori provvedimenti: la *Ley de Servicios de la Sociedad de Información y de Comercio Electrónico* (LSSI)[232] e la *Ley General de Telecomunicaciones* (LGT)[233], a cui poi si è aggiunto il *Real Decreto (RD) n. 424/2005.*

In generale, è stato osservato che la necessità di dare attuazione alle diverse direttive comunitarie ha fatto sì che la frammentazione normativa sia diventata una costante dell'ordinamento spagnolo[234].

L'Agenzia per la protezione dei dati[235] è l'organo pubblico indipendente preposto alla vigilanza del settore relativo alla protezione dei dati personali, al quale sono demandate tutta una serie di attività funzionali all'applicazione della legge: rilasciare le autorizzazioni necessarie, esaminare i reclami degli interessati, eseguire ispezioni sugli archivi oggetto della legge organica, l'emanazione delle sanzioni. Mentre, in Catalogna e nella Comunità autonoma di Madrid sono presenti due omologhe autorità autonomiste.

5.2. La Francia

Anche in Francia la protezione della riservatezza è stata il risultato di un processo lungo in cui prima la dottrina e successivamente la giurisprudenza hanno avuto un ruolo molto importante.

---

[231] Consultabili su https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/index-ides-idphp.php

[232] legge n 34/2002, consultabile anche con le successive modifiche su http://www.mityc.es/dgdsi/lssi/normativa/ Paginas/normativa.aspx

[233] Legge n 32/2003, modificata da ultimo il 10/12/2010, vedi http://www.mityc.es/es-ES/GabinetePrensa/NotasPrensa/2010/Paginas/npanteproyectolgt101210.aspx

[234] Così D. GRAMUNT FOMBENA, *Dati personali e comunicazioni elettroniche. L'attuazione della direttiva CE N- 2002/58 nell'ordinamento spagnolo*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Il codice del trattamento dei dati personali, Giappichelli, Torino, 2007, pag 948, a cui si rinvia.

[235] https://www.agpd.es/portalwebAGPD/conozca/index-ides-idphp.php

In particolare negli anni sessanta i giudici ordinari francesi, in assenza di una legge o di una norma costituzionale che prevedessero un autonomo diritto alla *vie privée*, hanno elaborato un insieme di misure volte a tutela della riservatezza dei singoli: un'autentica *création prétorienne* di diritto non scritto[236].

Su questa linea la Francia ha avviato in seguito una modifica legislativa che ha portato alla positivizzazione del diritto alla vita privata[237] . E' merito, però, del Conseil constitutionnel aver elevato, attraverso un'operazione ermeneutica, il diritto alla *vie privée* al rango di diritto costituzionale. Con la sentenza n. 94-352 DC del 18 gennaio 1995, i giudici costituzionali francesi hanno riconosciuto, infatti, espressamente il diritto costituzionale alla vita privata, fondandone la tutela sulla libertà prevista dall'art 2 della Dichiarazione dei diritti dell'uomo e del cittadino del 1789[238].

E', invece, del 6 gennaio 1978 la legge 78-17 sulla protezione dei dati, legge che tra l'altro è stata in Europa una delle prime in materia.

Tale normativa trae origine dalla divulgazione nel 1974 sulla stampa francese di un progetto volto a collegare tutti i file dell'amministrazione ad un numero unico di identificazione dei cittadini (conosciuto con il nome di *progetto SAFARI*). Questo creò una certa preoccupazione nell'opinione pubblica e così venne formato un Comitato responsabile di effettuare proposte, per garantire che lo sviluppo tecnologico fosse fatto nel rispetto della vita privata, le libertà fondamentali.

Proprio su raccomandazione dal Comitato, il 6 gennaio 1978 è stata approvata la *Loi informatique e libertés* e istituita un'autorità indipendente per garantirne l'effettività, la *Commission Nationale de l'Informatique e des Libertés* (CNIL)[239]

Nonostante ciò o forse per questo motivo la Francia è stata, invece, l'ultimo paese a dare attuazione alla Direttiva n. 95/46, con legge del 6 agosto 2004, che ha modificato la legge del 6 gennaio 1978[240].

---

[236] Così C. SARTORETTI, *Contributo allo studio del diritto alla privacy nell'ordinamento costituzionale. Riflessioni sul modello francese*, Giappichelli, 2008, pag. 45.

[237] Segnatamente con la modifica dell'art 9 del Code Civil e con la legge 17 luglio n 643 artt. 22 e 23.

[238] In Rev. Fr de dr constitutionnel 1995, pp. 350 ss. Cfr. anche C. SARTORETTI, *Contributo allo studio del diritto alla privacy nell'ordinamento costituzionale. Riflessioni sul modello francese*, op cit,

[239] http://www.cnil.fr/

[240] http://www.cnil.fr/index.php?id=45

Questo ritardo ha comunque fatto sì che, come il nostro Codice, anche la legge francese appaia molto moderna nel suo impianto, avendo fatto tesoro degli sviluppi nel frattempo intercorsi e delle diverse applicazioni giurisprudenziali intervenute.

Questo si evidenzia, ad esempio, nel principio della responsabilità anche delle imprese nell'attuazione della legge (riconoscimento dell'autoregolamentazione), ma anche dei cittadini nella tutela dei loro diritti.

Sono state prese in considerazione poi tutte le possibilità di semplificazione, così com'è stata prevista l'istituzione in seno alle imprese di corrispondente alla protezione dei dati personali[241].

Inoltre, l'evoluzione che forse maggiormente deve essere sottolineata è quella finalizzata ad armonizzare il cd. *controllo preventivo* alla creazione di trattamenti, che è sempre stato la modalità d'azione privilegiata de la CNIL, e il *controllo successivo*, in particolare attraverso l'istituzione di denunce, controlli e, qualcosa di totalmente nuovo, l'esercizio dei poteri sanzionatori.

La legge francese sulla protezione dei dati personali ha una portata molto ampia, copre, infatti, tutti i settori di attività di trattamento dei dati, inclusi quelli operati negli ambiti della sicurezza pubblica, della difesa e in materia penale. Si applica ai trattamenti automatizzati, quanto a quelli operati manualmente. Non si applica, invece, come previsto dalla direttiva, ai trattamenti finalizzati ad una attività puramente personale.

Le definizioni dei termini chiave della protezione dei dati rispecchiano quelle indicate nella direttiva[242].

Riguardo al CNIL, questa oltre ad essere la più antica Autorità garante della protezione dei dati personali è anche la prima delle cd. Autorità amministrative indipendenti francesi. E' un organo collegiale composto da 17 membri ed ha il compito di garantire il rispetto dei diritti e delle libertà delle persone, vigilando che il trattamento dei dati personali avvenga secondo i principi stabiliti dalla legge.

---

[241] Cfr. G. MATHIAS, *La legge <<Informatique et Libertés>>: un quadro giuridico rinnovato per la tutela dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Il codice del trattamento dei dati personali, op. cit. pag 931 e ss.

[242] Per un approfondimento sulla legge n. 2004-801 del 2004 si veda anche G. MATHIAS, *La legge <<Informatique et Libertés>>: un quadro giuridico rinnovato per la tutela dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Il codice del trattamento dei dati personali, op. cit. pag 923 e ss.

Oltre a ciò, agendo in un contesto tecnico in costante evoluzione la stessa è tenuta a seguire attentamente gli sviluppi delle tecnologie e le conseguenze che queste possono avere per i diritti umani, la privacy e le libertà fondamentali.

In tal modo, le suddette funzioni dell'Autorità francese finiscono per essere così rilevanti, ai fini della più efficace garanzia del diritto alla protezione dei dai personali, da far ritenere che "se (…) la legge 6 agosto 2004 riafferma i principi della protezione dei dati personali, da tempo assunti tra i principi fondamentali dell'ordinamento francese, ciò si deve anche al ruolo esercitato dalla CNIL e alla costante opera di vigilanza che essa svolge, attraverso i suoi pareri e le sue decisioni, sul rispetto di tali principi con riferimento ai continui sviluppi tecnici"[243]

5.3. La Gran Bretagna

Anche in Gran Bretagna il diritto ala privacy è nato e si è sviluppato soprattutto ad opera dei giudici, i quali hanno costruito singoli rimedi rispetto alla molteplicità delle situazioni giuridiche portate alla loro attenzione[244].

L'espansione delle nuove tecnologie e la conseguente evoluzione del concetto di privacy hanno reso, tuttavia, necessario l'intervento legislativo.

Dal 1 Marzo 2000 la tutela dei dati personali in Gran Bretagna è disciplinata dal *Data Protection Act* 1998[245], in attuazione della Direttiva n. 95/46/CE . La nuova legge, che è completata da ben 17 regolamenti di attuazione, ha rafforzato ed esteso il regime di tutela dei dati personali che in Gran Bretagna era previsto sin dal *Telecommunications and Data Protection Act* del 1984.

---

[243] G. MATHIAS, *La legge <<Informatique et Libertés>>: un quadro giuridico rinnovato per la tutela dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Il codice del trattamento dei dati personali, op. cit. pag 944..

[244] Ad esempio il *trepass*, utilizzato in caso di acquisizione di informazioni sulla vita privata altrui mediante l'invasione o la violazione del diritto di proprietà o altro diritto dell'interessato, il *brech of trust* o *confidence*, finalizzato a tutelare il riserbo su informazioni confidenziali. Cfr. C. SARTORETTI, *Contributo allo studio del diritto alla privacy nell'ordinamento costituzionale. Riflessioni sul modello francese*, op cit, pag 42 e ss; A. CERRI, *voce Riservatezza (diritto alla), III) Diritto comparato e straniero*, in Enc. Giur. Treccani, Istituto Poligrafico e Zecca dello Stato, Roma 1995.

[245] http://www.statutelaw.gov.uk/content.aspx?LegType=All+Primary&PageNumber=1&BrowseLetter=D&NavFrom=1&activeTextDocId=3190610&parentActiveTextDocId=3190610&showAllAttributes=0&hideCommentary=0&showProsp=0&suppressWarning=1, questa versione include le modifiche introdotte successivamente.

In particolare, l'ambito di applicazione della legge è stato esteso anche a certe forme di archivi manuali, mentre il *data subject* (ovvero il soggetto cui si riferiscono i dati personali) gode di una tutela più ampia e le procedure di registrazione sono state sostituite con procedure di notificazione.

Sono stati poi riaffermati i principi di qualità nel trattamento, sono state previste condizioni più stringenti per il trattamento di certi dati particolari (ad esempio quelli "sensibili") insieme a nuove regole per il trasferimento dei dati a Paesi fuori dall'UE.

Infine, sono stati rafforzati i poteri dell'Autorità garante. Questa è stata originariamente denominata *Data Protection Registrar* (1984), poi *Data Protection Commissioner* (1998) e, dal 30 gennaio 2001, *Information Commissioner*[246].

L'*Information Commissioner* è un'autorità pubblica indipendente, risponde, infatti, della sua attività solo nei confronti del Parlamento britannico, al quale è obbligato periodicamente a riferire su quanto compiuto in adempimento dei suoi doveri di vigilanza e interpretazione del *Data Protection Act e* delle leggi affini, come la legge del 2004 sulle informazioni ambientali e la segretezza delle comunicazioni elettroniche del 2003.

Nel *Data Protection Act* sono stati stabiliti, poi, i principi cardine per l'elaborazione dei dati personali, a cui tutti gli utilizzatori di dati devono conformarsi incondizionatamente; tali principi, che vengono dettagliatamente specificati dal "Garante" nel corso della propria attività di interpretazione e adeguamento della disciplina, sono sorretti da sanzione penale per omissione da chiunque compiuta.

Tuttavia, si evidenzia anche che la disciplina non si applica ai trattamenti di dati personali effettuati per la sicurezza nazionale, la prevenzione o la repressione del crimine, la valutazione o determinazione della tassazione nazionale e per gli scopi specifici dell'amministrazione statale.

Inoltre, si è osservato che in generale la disciplina legislativa inglese è focalizzata sulla figura del responsabile del trattamento dei dati personali, piuttosto che sull'esercizio del controllo da parte della persona interessata. Per questo motivo, le regole vigenti non sono riuscite a coinvolgere

[246] http://www.ico.gov.uk/.

particolarmente l'opinione pubblica e non sono generalmente considerate come lo strumento ordinario per la tutela della privacy individuale.

Al riguardo, le stesse corti tendono a rifiutare l'idea che il diritto alla privacy possa costituire nel diritto inglese fondamento di una distinta azione di giudizio, preferendo adattare l'applicazione di altre azioni già esistenti, soprattutto quella esperibile in *equity* di *breach of confidence*[247].

Quanto alla tutela giurisdizionale ordinaria, si segnala, che in Inghilterra viene esercitata dal Tribunale di primo livello (*Information Rights*)[248], il quale è composto di membri togati e non togati ed è competente, inoltre, a conoscere i reclami avverso le decisioni dell'Information Commissioner.

In riferimento alla Gran Bretagna, si evidenzia infine che nell'aprile 2009 l'Unione europea ha aperto una procedura di infrazione nei confronti del Paese per violazione delle leggi comunitarie sulla privacy[249].

La società Phorm avrebbe, infatti, fornito alla British Telecom[250]una tecnologia in grado di convertire le informazioni sulle abitudini on line degli utenti in elementi utili per campagne di marketing e promozioni commerciali, fornendo agli stessi utenti una "pubblicità su misura".

Come spiegato dal commissario Viviane Reding[251] "Le tecnologie come il *behavioural advertising* possono essere utili alle aziende e ai clienti, ma devono essere utilizzate nel rispetto della normativa europea. Queste norme esistono per proteggere la privacy dei cittadini e devono essere applicate in maniera rigorosa da tutti gli Stati membri. Seguiamo il caso Phorm da diverso tempo e abbiamo concluso che vi sono dei problemi nel modo in cui il Regno Unito ha applicato parti della normativa europea in materia di riservatezza delle comunicazioni. Invito le autorità britanniche a modificare la legislazione nazionale e a far sì che le autorità dispongano dei poteri

[247] In tal senso si rinvia alle osservazioni di I. WALDEN, *Data protection nel Regno Unito*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Il codice del trattamento dei dati personali, op. cit., pag. 992 e ss.

[248] The First-tier Tribunal (Information Rights) è stato costituito nel 2000, inizialmente come il Data Protection Tribunal, è stato in seguito ribattezzato Information Tribunal e il 18 gennaio 2010 è stato trasferito nella General Regulatory Chamber of the First-tier Tribunal . Il suo sito web ha i dettagli della procedura di ricorso, i collegamenti alla specifica normativa, comprese le norme procedurali, un elenco dei ricorsi pendenti ("casi in corso"), e delle decisioni dal 2000 in poi in versione integrale. Vedi http://www.informationtribunal.gov.uk/

[249] Cfr http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570&format=HTML&aged=0&language=IT&guiLanguage=en

[250] http://www.ilsole24ore.com/art/SoleOnLine4/Finanza%20e%20Mercati/2010/02/scheda-britishtelecom.shtml?uuid=6e7a1eae-224c-11df-bc23-7e37ad467041&DocRulesView=Libero

[251] Vedi nota 249.

necessari per comminare sanzioni al fine di attuare la normativa dell'UE in materia. In questo modo il Regno Unito potrà rispondere più energicamente alle nuove sfide legate alla *ePrivacy* e alla tutela dei dati personali, come quelle poste dal caso Phorm, e i consumatori britannici sapranno che la loro privacy e i loro dati sono protetti quando navigano in internet "[252].

5.4. La Germania

Anche l'esperienza tedesca in materia è segnatamente caratterizzata dall'importanza del ruolo avuto dalla giurisprudenza e, in particolare, dalla giurisprudenza costituzionale, la quale, insieme alla dottrina, si è proposta per molto tempo di cercare un fondamento costituzionale del diritto alla privacy.

Fra le sentenze del Tribunale federale costituzionale tedesco, merita particolare attenzione la cd. "decisione sul censimento" del 1983 (Volkszählunentscheidung)[253], in quanto è considerata pietra miliare nella storia della disciplina dei dati personali, anche al di fuori della Germania.

Il giudice costituzionale tedesco, infatti, si è accorto con notevole lungimiranza, rispetto ad altre Corti costituzionali, di quali avrebbero potuto essere le ripercussioni di intensi e generalizzati processi di trattamento di dati personali sulle libertà individuali.

In particolare, a quel tempo l'opinione pubblica era concentrata sulla "legge sul censimento per il 1983". Questa aveva sollevato molte critiche non solo da pare della società, ma anche dalle autorità federali e statali di protezione dei dati personali.

Davanti al BVerG sono stati presentati così più 1300 ricorsi! Non sorprende, quindi, che Il Tribunale federale abbia esteso l'oggetto della sua pronuncia, finendo per occuparsi non solo della legge impugnata[254], ma

[252] Una rassegna dettagliata dei procedimenti di infrazione nel settore delle telecomunicazioni è disponibile alla pagina: http://ec.europa.eu/information_society/policy/ecomm/implementation_enforcement/infringement/

[253] NYW, 1984, pag 420 e ss. Cfr A. DI MARTINO, *La protezione dei dati personali*, in S. P. PANUNZIO (a cura di), I diritti fondamentali e le corti in Europa, Jovine, 2005 pag. 386 e ss.; C.SARTORETTI, *Contributo allo studio del diritto alla privacy nell'ordinamento costituzionale*, op cit. pag 44.

[254] In particolare sulla dichiarazione di illegittimità costituzionale del § 9 nella parte in cui prescriveva il collegamento tra finalità statistiche e amministrative dei dati raccolti con il censimento. Secondo A. DI MARTINO, ult.. op. cit.: " Da un punto di vista processuale, la decisione merita di essere ricordata non

anche dei principi in materia di tutela dei dati personali che fosse possibile dedurre dalle norme costituzionali.

Con la sentenza citata, il BVerfG ha attribuito inequivocabilmente alla tutela dei dati personali un rilievo costituzionale, attraverso l'individuazione di un *Recht auf informationelle Selbustberstimmung*, ovvero di un diritto all'autodeterminazione informativa, ricostruito come concretizzazione del diritto generale della personalità di cui agli artt. 1, comma 1 e 2 comma 1 della Costituzione. Il suo contenuto è individuato nel "potere di ciascuno di decidere sostanzialmente da sé circa la rivelazione e l'utilizzo dei propri dati personali".

Importante, inoltre, è la dimensione sociale affidata a questo diritto. La Corte, infatti, ha sviluppato il concetto di autodeterminazione individuale quale presupposto per l'esercizio delle libertà democratiche. Esso risulta gravemente inibito dalla non conoscenza della sorte delle informazioni personali cedute dagli individui. Chi ignora cosa verrà raccolto e da chi non sa quali comportamenti può legittimamente tenere e, temendo che alcuni fatti siano schedati, rinuncia ad esempio a partecipare ad assemblee, manifestazioni, riunioni sindacali, cioè all'esercizio di diritti costituzionali.

Questo avrebbe conseguenze non solo sul suo sviluppo personale, ma anche su quello collettivo, poiché l'autodeterminazione è una condizione elementare che si basa sulla possibilità di agire e coagire dei cittadini e quindi sulla democrazia.

Il libero sviluppo della personalità presuppone la protezione del singolo dalla memorizzazione, utilizzazione e trasferimento incontrollato di dati personali[255].

---

solo per questa non ortodossa estensione del *thema decidendum*, ma anche perché è stata emessa sulla base di una cd *Rechtssatzverfassungbeschwerde*, ossia un ricorso diretto avente ad oggetto una norma di legge, ammesso solo in ipotesi particolarmente restrittive." Per quest'ultimo aspetto si rinvia a J. LUTHER, R. ROMBOLI, R. TARCHI, *Esperienze di giustizia costituzionale*. Tomo I. Usa, Canada, Svizzera, Austria, Germania, Francia, Giappichelli, Torino, 2000.

[255] "Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit uber sie weiß. Wer unsicher ist , ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wirdversuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies wurde nicht nur die individuellen Entfaltungschancen des einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs – und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist", citazione in lingua originale da M. PROSPERI, *il diritto alla riservatezza nell'ordinamento costituzionale,* op. cit.

Inoltre, dal giudice costituzionale tedesco sono stati tracciati anche i confini del diritto fondamentale all'autodeterminazione informativa, allorché ha affermato che questo trova limite unicamente nella legge. Un provvedimento legislativo può, dunque, porre limiti al diritto in oggetto attraverso l'esplicita indicazione sia dei requisiti di tali limitazioni, sia del grado della loro intensità.

Tuttavia, ogni intervento legislativo deve ispirarsi al principio di proporzionalità tra mezzo applicato e finalità perseguita[256].

La raccolta dei dati e la loro elaborazione, inoltre, sono consentite soltanto nei casi in cui questi processi avvengono in un legame stretto con una finalità concreta e lecita. "Questo principio di connessione tra la raccolta dei dati e scopo (*Zweckbindung*) è una delle colonne portanti della disciplina tedesca"[257].

Per quanto riguarda la normativa, fin dagli anni settanta la Germania possiede un'ampia disciplina in materia di privacy e trattamento personale sia a livello federale che di singoli Lander. I Lander dell'Assia e della Renania Palatinato, infatti, già rispettivamente nel 1970 e 1974 si sono muniti di una normativa e hanno previsto un'autorità garante eletta dal Parlamento[258].

Il Parlamento federale, invece, ha adottato nel 1977 il *Bundesdatenschtuzgesetz*, a cui sono succedute la legge del 1990 e il BDSG del 2001, che ha attuato la Direttiva n. 95/46, quest'ultima ampiamente modificata nel luglio 2009[259].

Le modifiche sono state finalizzate a "limitare il commercio illegale di dati personali" e hanno dato maggior interesse al controllo sul trattamento dei loro dati personali[260]. Ad esempio, i poteri di controllo delle autorità di protezione dei dati sono stati aumentati, per il trattamento dei dati con

[256] F. A. SCHURR, *La tutela dei dati personali nell'esperienza tedesca*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Il codice del trattamento dei dati personali, op. cit.. pag 978

[257] Così F. A. SCHURR, *La tutela dei dati personali nell'esperienza tedesca*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Il codice del trattamento dei dati personali, op. cit.. pag. 978.

[258] Per le leggi dei singoli Lander, vedi http://ec.europa.eu/justice/policies/privacy/law/implementation_en.htm#italy e http://www.privacy.it/l inkpriv1.html.

[259] http://translate.googleusercontent.com/translate_c?hl=it&langpair=en|it&u=http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf%3F__blob%3DpublicationFile&rurl=translate.google.it&usg=ALkJrhg9II0xZk6szorFjxVGtoOnhOpeQw.

[260] Cfr http://translate.google.it/translate?hl=it&langpair=en|it&u=http://www.stbdirectmarketing.com/german-data-protection.aspx.

finalità di marketing si è passati dal paradigma dell'*opt out* al *opt in*, è stato introdotto un livello maggiore di protezione per i dati dei lavoratori e sono aumentate le sanzioni in caso di violazione della legge.

Nel complesso, il sistema tedesco si basa sul cd. divieto con riserva di permesso, secondo il quale il trattamento dei dati personali, tendenzialmente vietato, è consentito in presenza di precisi presupposti di carattere sostanziale, come il consenso dell'interessato, il prevalente interesse del responsabile del trattamento o quello generale[261].

Il diritto tedesco opera poi una distinzione relativamente alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, a seconda che detto trattamento sia effettuato da organismi pubblici o meno.

Le autorità incaricate di vigilare sul rispetto delle disposizioni in materia, da un lato, da parte degli organismi pubblici e, dall'altro, da parte degli organismi diversi da quelli pubblici e delle imprese di diritto pubblico che partecipano alla concorrenza sul mercato (*öffentlich-rechtliche Wettbewerbsunternehmen*), sono infatti distinte.

Sul trattamento dei dati personali da parte degli organismi pubblici vigilano, a livello federale, il *Bundesbeauftragter für den Datenschutz und die Informationsfreiheit* (Incaricato federale per la protezione dei dati e la libertà dell'informazione)[262] e, a livello dei Länder, i *Landesdatenschutzbeauftragte* (Incaricati per la protezione dei dati dei Länder)[263].

Tali organismi sono tutti responsabili solamente nei confronti dei rispettivi Parlamenti e di norma non sono sottoposti ad alcuna vigilanza, istruzioni o altra influenza da parte degli organismi pubblici che sono soggetti al loro controllo.

Per contro, la struttura delle autorità incaricate di sorvegliare il trattamento dei dati in parola da parte dei settori diversi da quello pubblico varia da un Land all'altro[264].

---

[261] A. DI MARTINO, *La protezione dei dati personali*, in S. P. PANUNZIO (a cura di), I diritti fondamentali e le corti in Europa, op. cit., pag. 420 e 386 e ss.

[262] www.bfdi.bund.de

[263] https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Datenschutzbeauftragte/Datenschutzbeauftragte.php

[264] Si evidenzia, tra l'altro, che Le leggi dei Länder hanno tuttavia la caratteristica comune di assoggettare espressamente dette autorità di controllo ad una forma di vigilanza dello Stato. Tuttavia, la Commissione europea ha ritenuto questo incompatibile con le previsioni indicate dalla Direttiva n. 95/46 (art. 28, n. 1, secondo comma) e il 5 luglio 2005 ha inviato una lettera di diffida alla Repubblica federale di Germania. Quest'ultima ha risposto con una lettera del 12 settembre 2005, affermando che il sistema tedesco di vigilanza in materia soddisfa i requisiti della direttiva in parola. Il 12 dicembre 2006, la

Commissione ha inviato un parere motivato alla Repubblica federale di Germania, ribadendo la censura formulata in precedenza.

Nella sua risposta del 14 febbraio 2007, lo Stato ha confermato il suo punto di vista iniziale. La Commissione ha, quindi, deciso, di proporre ricorso alla Corte di Giustizia. Secondo quest'ultima: "La garanzia dell'indipendenza delle autorità nazionali di vigilanza è diretta ad assicurare l'efficacia e l'affidabilità del controllo del rispetto delle disposizioni in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali e deve essere interpretata alla luce di tale finalità. Essa non è stata disposta al fine di attribuire uno status particolare a dette autorità ed ai loro agenti, bensì per rafforzare la protezione delle persone e degli organismi interessati dalle loro decisioni. Ne discende che, nello svolgimento delle loro funzioni, le autorità di controllo devono agire in modo obiettivo ed imparziale. A tale fine esse devono essere sottratte a qualsiasi influenza esterna, compresa quella, diretta o indiretta, dello Stato o dei Länder, e non solamente essere poste al riparo dall'influenza degli organismi controllati." Pertanto la Corte ha statuito che la Germania ha violato gli obblighi imposti dalla suddetta normativa comunitaria, con sentenza del 9 marzo 2010, causa C-518/07, GUUE C 113/4 del 1 maggio 2010, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:113:0003:0004:IT:PDF e integrale su http://eur-lex.europa.eu/Notice.do?mode=dbl&lang=en&ihmlang=en&lng1=en,it&lng2=da,de,en,et,fi,fr,it,mt,nl, pl,ro,sk,sl,sv,&val=509216:cs&page=.

CAPITOLO SECONDO

Privacy e nuove tecnologie: sanità elettronica, e-government, comunicazioni elettroniche, biometria e sicurezza

SOMMARIO: 1. Classificazione delle tecnologie rispetto agli interventi regolatori. – 2. Privacy e Sanità elettronica. - 2.1. Dalle cartelle cliniche cartacee, alle cartelle elettroniche locali fino al fascicolo sanitario elettronico. - 2.2. I referti on line. - 2.3. La telemedicina. - 2.4. I dati genetici. – 3. Privacy e E-government. - 3.1. Quadro normativo ed istituzionale. - 3.2. Tutela dei dati personali e sicurezza informatica nell'amministrazione digitale. - 3.3. La posta elettronica certificata (PEC) e le carte elettroniche. - 3.3.1. La posta elettronica certificata (PEC). - 3.3.2. Le carte elettroniche. - 3.4. Privacy e diritto di accesso nella p.a. digitale. - 3.5. L'accessibilità in rete dei dati: il caso della pubblicazione on line delle dichiarazioni dei redditi. – 4. Privacy e Comunicazioni elettroniche. - 4.1. Internet. - 4.1.1. Quadro giuridico di riferimento. - 4.1.2. Anonimato protetto. - 4.1.3. Responsabilità del provider, misure minime di sicurezza e documento programmatico di sicurezza. - 4.1.4. Furti d'identità. - 4.1.5. Lo spam. - 4.1.6. Privacy by design e social engineering. - 4.2. Tecnologia ubiquitous computing. - 4.2.1. La tecnologia Rfid. - 4.2.2. La geolocalizzazione. – 5. Privacy e tecnologie biometriche. 6. Privacy e sicurezza: la questione dei body scanners ed il caso PNR (Passenger Name Record). - 6.1. I body scanners. - 6.2. Il caso PNR (Passenger Name Racord).

1. Classificazione delle tecnologie rispetto agli interventi regolatori

Il settore delle tecnologie è senza dubbio molto vasto e soprattutto caratterizzato da un dinamismo che mal si presta a schemi generalizzanti, tuttavia, sono state efficacemente evidenziate tre macro aree[265], tenendo in

[265] Così G. SANTANIELLO, *Tipologia delle innovazioni tecnologiche e protezione dei dati personali*, in Innovazione tecnologiche e privacy, op. cit.

considerazione gli interventi regolatori a vari livelli del rapporto fra privacy e nuove tecnologie:

1) il settore delle innovazioni tecnologiche che sono già ricomprese in un quadro di regole di valore legislativo che le governano;

2) il settore delle innovazioni tecnologiche inquadrabili finora in linee guida derivanti dal potere prescrittivo di carattere amministrativo (ad es. autorizzazioni generali, decaloghi di comportamento, etc.) oppure derivanti da codici deontologici e di buona condotta, formati con l'intervento dell'Autorità garante;

3) il settore delle innovazioni tecnologiche, che in relazione al loro recente sviluppo, non sono ancora sorrette da regole specifiche, né di valore legislativo né di un efficiente potere ordinatorio amministrativo.

Nella prima categoria rientrano le comunicazioni elettroniche, regolate sia a livello europeo (direttive europee del 2002 e 2006) sia nel diritto interno, dove assume particolare rilevanza il Codice delle comunicazioni elettroniche, D.lgs. n. 259/2003[266], il quale, garantendo in via di principio il diritto all'uso dei mezzi di comunicazione elettronica, stabilisce anche che "sono fatte salve le limitazioni derivanti da esigenze (...) della riservatezza e protezione dei dati personali".

Inoltre, lo stesso prevede che, in caso di conflitto fra il diritto di iniziativa economica nel campo delle comunicazioni elettroniche e le normative a protezione della vita privata e dei dati personali, prevalgano queste ultime.

Il secondo settore comprende un vasto numero di tecnologie di tipo diverso quali, ad esempio, le tecniche biometriche ed il trattamento dei dati genetici.

Nonostante manchi per tali tipi di trattamento un *corpus* legislativo, l'Autorità garante ha emanato linee guida di tipo amministrativo, autorizzazioni generali, decaloghi di comportamento, elaborando parametri per la legittimità e la correttezza dei trattamenti.

In quest'ambito, poi, i codici deontologici occupano una posizione rilevante. Come in precedenza accennato, questi atti nascono dal coordinamento fra poteri propulsivi e di indirizzo del Garante e la

[266] Consultabile su http://www.parlamento.it/parlam/leggi/deleghe/03259dl.htm.

proposizione delle regole da parte dei soggetti rappresentativi di determinate categorie.

Infine, il terzo settore ricomprende tecnologie di ultimissima generazione, spesso ancora in fase di sperimentazione, le quali, tuttavia, già si pongono all'attenzione, oltre che per la notevoli opportunità che possono realizzare, anche per nuove vulnerabilità individuali e sociali[267] che allo stesso tempo possono creare.

Tra queste rientrano le tecnologie Rfid, come le etichette intelligenti che potrebbero presto sostituire i classici codici a barre, consentendo, come si vedrà più avanti nella trattazione, di seguire i prodotti nei loro spostamenti, con la possibilità però anche di controllare coloro che hanno acquistato o usano tali prodotti.

2. Privacy e Sanità elettronica

Nell'ambito della più ampia categoria dei dati cd. "sensibili" (art. 4 let d) D.lgs. n. 196/03), riguardanti cioè profili particolarmente delicati della vita privata e delle persone (es. sfera religiosa, politica, sindacale e filosofica, origine razziale ed etnica), le informazioni relative allo stato di salute e alla vita sessuale, proprio per l'intrinseca attinenza alla sfera più intima della persona, sono state oggetto di una speciale protezione, contenuta nel Titolo V del D.lgs. n. 196/03.

Queste informazioni possono essere trattate per fini di ricerca medica e scientifica, spesso, con l'obiettivo di individuare metodologie che assicurino la prevenzione di patologie e l'integrità fisica o psichica non solo della singola persona cui i dati si riferiscono, ma dell'intera collettività.

Di frequente, inoltre, gli atti e i documenti nei quali sono riportati i dati sulla salute sono raccolti e predisposti per scopi amministrativi - ad esempio, il riconoscimento di particolari benefici (come l'esenzione dal ticket) - per l'accertamento di responsabilità o per il risarcimento dei danni.

Paradossalmente questa tendenza si è accentuata con la crisi del cd. Welfare di massa. Il Welfare cd. selettivo, infatti, ha bisogno di

[267] Così G. SANTANIELLO, *Tipologia delle innovazioni tecnologiche e protezione dei dati personali*, op. cit.

informazioni personali sempre più analitiche per consentire l'accesso a determinati servizi[268].

Come fonte integrativa della disciplina applicabile ad alcuni trattamenti di dati sensibili, il Codice della privacy ha confermato lo strumento delle autorizzazioni generali, che consentono al titolare del trattamento di derogare all'obbligo di presentare al Garante una richiesta di autorizzazione, se il trattamento è conforme alle relative prescrizioni (art 40 cc 1 e 2 del Codice).

Per quanto riguarda il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, l'autorizzazione ad oggi di riferimento è la n. 2/2009[269].

Considerata "la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e, in particolare, per il diritto alla protezione dei dati personali sancito dall'art. 1 del Codice, principi valutati anche sulla base delle raccomandazioni adottate in materia di dati sanitari dal Consiglio d'Europa ed in particolare dalla Raccomandazione N. R (97) 5, in base alla quale i dati sanitari devono essere trattati, di regola, solo nell'ambito dell'assistenza sanitaria o sulla base di regole di segretezza e di efficacia pari a quelle previste in tale ambito"[270], l'autorizzazione n. 2 /2009 è finalizzata, appunto, a consentire il trattamento ai soggetti in essa individuati, prescrivendo misure uniformi a garanzia degli interessati, rendendo così non necessaria la richiesta di singoli provvedimenti autorizzatori[271].

Il trattamento oggetto di autorizzazione può riguardare i dati strettamente pertinenti agli obblighi, ai compiti e alle finalità indicate che non possano essere adempiuti o realizzati, caso per caso, mediante il

[268] Secondo alcuni, il rischio sarebbe ancora maggiore se si imboccasse la strada della privatizzazione, per il pericolo di ledere fortemente il principio di uguaglianza: si avrà tanta salute quanto si sarà in grado di comprarla sul mercato, paventando così il ritorno ad una "cittadinanza censitaria", espressione usata spesso da Rodotà, vedi ad es. S. RODOTà, *Apologia dei diritti*, in Lezioni Noberto Bobbio, Torino 2004, consultabile su http://www.scribd.com/doc/53206551/Apologia-dei-diritti-Stefano-Rodota-I-diritti-dell-uomo-oggi-Norberto-Bobbio

[269] Autorizzazione n. 2/2009 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, 16 dicembre 2009, G.U. n. 13 del 18 gennaio 2010 - suppl. ord. n. 12, consultabile su http://www.garanteprivacy.it/garante/ doc.jsp?ID=1682956

[270] Autorizzazione 2/2009 cit.

[271] Vedi G. SANTANIELLO (a cura di), *La protezione dei dati personali* , op. cit., pag 494 ss

trattamento di dati anonimi o di dati personali di natura diversa, e può comprendere le informazioni relative a stati di salute pregressi.

Inoltre, già a monte del trattamento, i sistemi informativi e i programmi informatici devo essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possano essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

L'utilizzo, il trattamento e la circolazione dei dati personali in ambito sanitario crescono esponenzialmente con lo sviluppo delle applicazioni tecnologiche in questo settore.

La quantità e la complessità delle informazioni e delle conoscenze in campo sanitario sono aumentate al punto tale che la loro elaborazione rappresenta una funzione essenziale di qualsiasi struttura sanitaria. Quello della salute, infatti, è un settore che fa ampio ricorso alle informazioni e che dipende, quindi, in misura crescente dalle tecnologie dell'informazione e della comunicazione.

Per sanità elettronica si intende, appunto, l'applicazione di queste tecnologie all'intera gamma di funzioni che investono il settore sanitario, ad esempio, le reti di informazione sanitaria, le cartelle cliniche elettroniche, il fascicolo sanitario elettronico, i servizi di telemedicina, i sistemi di comunicazione personali portatili e indossabili, i portali salute e molti altri strumenti basati sulle tecnologie della comunicazione e dell'informazione e utilizzati per la prevenzione, la diagnosi, la cura, la sorveglianza sanitaria e la gestione dello stile di vita.

È innegabile il contributo, offerto da tali tecnologie alla ricerca medica, alla migliore gestione e diffusione delle conoscenze e all'affermazione di una medicina basata su prove di efficacia.

I mezzi offerti dalla sanità elettronica agevolano l'aggregazione, l'analisi e la memorizzazione di dati clinici in tutte le loro forme: gli strumenti di informazione consentono di accedere ai risultati più recenti, mentre gli strumenti di comunicazione rendono possibile una diffusa collaborazione tra organismi e professionisti del settore sanitario.

Tuttavia, è necessario che questa evidente potenzialità si sviluppi nel rispetto del diritto alla tutela dei dati personali che, come si è visto, in ambito sanitario sono particolarmente "sensibili". Questo fa della sicurezza un elemento essenziale dei sistemi informativi sanitari.

Rafforzare la fiducia, infatti, è un presupposto essenziale per lo sviluppo della società dell'informazione, a maggior ragione nel settore della sanità elettronica. I cittadini preferiscono poter fruire di servizi e informazioni, conformi alle loro esigenze e necessità, sentendosi nello stesso tempo tutelati sotto il profilo della privacy.

Per questo, in Italia è presente un Tavolo permanente per la Sanità elettronica[272], composto dai rappresentanti del Ministero per la Pubblica Amministrazione e l'Innovazione, del Ministero del Lavoro della Salute e delle Politiche Sociali, delle Amministrazioni Regionali e delle Province Autonome e coordinato dal Dipartimento per l'Innovazione e le Tecnologie.

Il TSE rappresenta la sede istituzionale di confronto e consultazione tra le Regioni, le Province autonome e l'Amministrazione Centrale per l'armonizzazione delle politiche tecnologiche della Sanità Elettronica e l'attuazione dei piani d'azione nazionale e regionali.

Anche in ambito comunitario è molto avvertita la necessità di sviluppare le tecnologie in ambito sanitario, in modo che i diversi sistemi introdotti nei diversi Stati siano in grado di dialogare fra loro, per consentire un'effettiva integrazione comunitaria in questo settore così delicato.

A tal fine nel 2004 la Commissione europea ha adottato l'*eHealth action plan*[273], contenente gli obiettivi in ambito di sanità elettronica da raggiungere entro il 2010[274].

Il piano ha invitato gli Stati a sviluppare strategie in grado di rispondere alle singole esigenze, pur in un costante reciproco dialogo, in modo che tutti i cittadini possano beneficiare di servizi più affidabili ed efficienti all'interno di uno "spazio europeo della sanità elettronica".

---

[272] http://www.sanitaelettronica.gov.it/se/.

[273] http://eurlex.europa.eu/Notice.do?mode=dbl&lang=en&ihmlang=en&lng1=en,it&lng2=da,de,el,en,es,fi,fr,it,nl,sv,&val=358060:cs&page=.

[274] In tal senso si vedano anche le conclusioni della conferenza *eHealth 2010*, tenuta a Barcellona dal 15 a 18 marzo 2010, http://ec.europa.eu/information_society/activities/health/policy/ehealth_conf/index_en.htm.

Sulla base di questo piano, il TSE ha emanato nel marzo 2005 un documento chiamato "Una politica per la Sanità Elettronica" e successivamente, nel marzo 2006 un altro documento, "Strategia architetturale per la Sanità Elettronica"[275]. Quest'ultimo, in particolare, ha indicato le politiche di privacy e la sicurezza del sistema complessivo come un aspetto centrale per l'intero sistema di sanità elettronica.

Centralità più volte ribadita dallo stesso Garante della privacy: "Lo sviluppo delle nuove tecnologie dell'informazione e delle comunicazione in campo sanitario esprime l'esigenza inderogabile di conciliare il valore dell'efficienza con l'altrettanto fondamentale valore della tutela della riservatezza dei cittadini. Il sistema di sanità elettronica, ancor più di altri, deve essere in grado di ingenerare la fiducia dei cittadini"[276].

La cd. "sanità elettronica" è un settore, quindi, particolarmente attuale e proprio in ragione della sua rilevanza, in termini anche di incidenza sull'economicità della spesa, è anche inserita negli obiettivi principali del piano governativo denominato e-gov 2012[277].

Alla luce di quanto evidenziato, per coniugare lo sviluppo delle tecnologie dell'informazione e la tutela della privacy nel settore sanitario non sembra potersi prescindere da alcuni principi guida. Tali principi sono già presenti all'interno del Codice in materia di protezione dei dati personali e sono suscettibili di differenti specificazioni, in relazione alle diverse applicazioni tecnologiche. In particolare, questi possono essere indicati in:

- garanzia dell'autodeterminazione dell'individuo: ad esempio con la possibilità di prenotare una visita medica o un esame specialistico anche attraverso sistemi tradizionali.
- Garanzia di un consenso informato e consapevole: è necessario informare adeguatamente l'interessato, anche in forma semplificata, sull'uso che verrà fatto dei suoi dati personali e dei trattamenti effettuati.

[275] http://www.sanitaelettronica.gov.it/se/documenti/TSE-IBSE-Strategia_architetturale-v01.00DEF.pdf

[276] G. CHIARAVALLOTTI, vice presidente dell'Autorità, in http://www.garanteprivacy.it/garante/doc.jsp?ID=1278064.

[277] Cfr http://www.governo.it/governoinforma/dossier/piano_e_gov_2012/.

- Adozione di misure di sicurezza a protezione dei dati, affinché si riducano i rischi di distruzione, perdita o accesso non autorizzato ai sistemi informatici e quindi ai dati così delicati.
- Privilegiare, quando possibile, la trasmissione di informazioni anonime, così come prevedere tecniche di cifratura e codici identificativi per l'uso dei dati da parte di organismi ed operatori sanitari.[278]

2.1. Dalle cartelle cliniche cartacee, alle cartelle elettroniche locali fino al fascicolo sanitario elettronico

Riguardo alla tutela della privacy nella sanità, particolare attenzione ha meritato in questi anni la cartella clinica, disciplinata dal Codice in materia di protezione dei dati personali all'art 92 D.lgs. n. 196/03[279]. Nata come un insieme di appunti per ricordare e trasmettere messaggi ad altri sanitari, oggi la cartella clinica riveste un notevole ruolo documentativo[280].

La cartella clinica è un insieme di documenti nei quali viene registrato dai medici e dagli infermieri un complesso di informazioni (anagrafiche,

[278] http://sanita.istitutoprivacy.it/.

[279] Art. 92. Cartelle cliniche

1. Nei casi in cui organismi sanitari pubblici e privati redigono e conservano una cartella clinica in conformità alla disciplina applicabile, sono adottati opportuni accorgimenti per assicurare la comprensibilità dei dati e per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati, ivi comprese informazioni relative a nascituri.

2. Eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:

a) di far valere o difendere un diritto in sede giudiziaria ai sensi dell'articolo 26, comma 4, lettera c), di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile

[280] Dal punto di vista giuridico la qualificazione della c.c. varia a seconda che l'estensore sia un'istituzione pubblica o privata convenzionata oppure una struttura privata non convenzionata.

Nei primi due casi la cartella clinica viene considerata un atto pubblico (fa quindi piena prova sino a querela di falso) ed il medico che la redige è un pubblico ufficiale (eventuale applicabilità degli articoli del codice penale in tema di falsità in atti pubblici…ecc.). Vedi Corte di Cassazione, Sez. V penale - 24 maggio 2010, n. 19557, consultabile su http://www.gadit.it/aggiornamento.asp?id=2690&idAgg=2; Corte di Cassazione, Sez feriale penale, sent n. 42166/2008, consultabile su http://www.altalex.com/index.php?idnot=43919&idstr=20. Ancora "Le attestazioni contenute in una cartella clinica sono riferibili ad una certificazione amministrativa per quanto attiene alle attività espletate nel corso di una terapia o di un intervento, mentre le valutazioni, le diagnosi o comunque le manifestazioni di scienza o di opinione in essa contenute non hanno alcun valore probatorio privilegiato rispetto ad altri elementi di prova", Cass. Civ. - Sez. III – 12/5/2003, n. 7201.

sanitarie, diagnosi e anamnesi ecc), riguardanti un determinato paziente - nonché a volte anche altri soggetti per la menzione di patologie riferite ad individui diversi dal principale interessato - al fine di poter predisporre gli opportuni interventi medici e poterne usufruire anche per indagini di natura scientifica, statistica, medico-legale e per l'insegnamento.

Ai sensi dell'art 26 del Nuovo Codice di Deontologia Medica[281], la cartella clinica delle strutture pubbliche e private deve essere redatta chiaramente, con puntualità e diligenza, nel rispetto delle regole della buona pratica clinica e contenere, le attività diagnostico-terapeutiche praticate, oltre ad ogni dato obiettivo relativo alla condizione patologica e al suo decorso.

La cartella clinica deve registrare i modi e i tempi delle informazioni nonché i termini del consenso del paziente - o di chi ne esercita la tutela - alle proposte diagnostiche e terapeutiche; deve inoltre registrare il consenso al trattamento dei dati sensibili da parte dell'interessato, con particolare riguardo ai casi di arruolamento in un protocollo sperimentale.

La conservazione della cartella clinica deve essere illimitata nel tempo così come i relativi referti (circolare ministeriale del 19/12/1986, n. 61)[282], mentre il termine è 5 anni nel caso di preparati citologici ed istologici (D.P.C.M. 10/02/1984)[283] e di 20 anni per le radiografie.

Una delle problematiche di maggior interesse, relativa alla tutela dei dati idonei a rivelare lo stato di salute o la vita sessuale, riguarda l'accesso ai dati da parte di un terzo ed in particolare, appunto, l'accesso alle cartelle cliniche.

La previgente normativa e ora l'attuale D.lgs. n. 196/03, agli artt. 26, comma 4 lett. c, 60, 71 e 92, comma 2, utilizzano come parametro, ai fini del vaglio di ammissibilità della richiesta di accesso, il concetto del diritto cd. "del pari rango"[284]: cioè l'accesso è ammesso se "la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso

[281] www.medicitalia.it/public/.../file/CodiceDeontologiaMedica.pdf.

[282] Cfr. http://www.guidelegali.it/guida.aspx?id_articolo=2148&idsc=7&titolo=La+cartella+clinica; vedi anche L. BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), *Next Privacy*, RCS Etas,Milano, 2010, pag 204.

[283] Consultabile su http://www.edilportale.com/normativa/decreto-pres.-cons.-min./1984/indirizzo-e-coordinamento-dell-attivit%E0-amministrativa-delle-regioni-in-materia-di-requisiti-minimi_cc3ad47c-5e89-4954-82d86f323c92f7d3.html.

[284] Vedi la nota successiva.

(…) è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile".[285]

Come si è osservato, lo sviluppo delle tecnologie nell'organizzazione sanitaria pone costantemente di fronte all'esigenza di bilanciare le potenzialità insite nello strumento tecnologico - quali la possibilità non solo di avvicinare i cittadini al servizio sanitario, ma anche di innalzare la qualità dei servizi stessi - con la necessità di tutelare il rispetto della privacy, in un settore come quello della sanità dove si usano i dati più intimi delle persone.

Dalla classica cartella fisica, di cui si è parlato, si sta velocemente passando, infatti, alla cd. cartella clinica elettronica locale. La cartella clinica elettronica locale (*Elettronic Patient Record*) fornisce in formato elettronico le informazioni contenute precedentemente nella cartella clinica cartacea, informazioni disponibili a tutto il personale sanitario e ad altre istituzioni entrambi previamente autorizzati, tutte le volte in cui tali informazioni siano necessarie.

La possibilità di comprendere molti tipi di informazioni e la particolarità del supporto che le contiene mettono in evidenza all'attenzione il bisogno di garantirne la sicurezza.

Come già rilevato, quindi, pur garantendo la facilità di accesso per il paziente e i suoi delegati, la sicurezza rappresenta un ulteriore aspetto di

[285] In merito è intervenuto espressamente il Garante il 9 luglio 2003 con un provvedimento generale (consultabile su www.garanteprivacy.it [doc.web n. 29832])sui diritti di "pari rango" a seguito di numeri quesiti, per verificare entro quali limiti persone diverse dagli interessati possano accedere ai dati sanitari ed in particolare alle cartelle cliniche. Si vedano anche i provvedimenti: 17 settembre 2009 [doc. web. 1656642], relativo alla cartella clinica del defunto e diritti del convivente, e 25 settembre 2008 [doc. web. 1555676], relativo alla cartelle cliniche dei defunti e all'accesso dei familiari.

La giurisprudenza amministrativa si è orientata nel senso di ritenere che la disposizione, applicata alla materia dell'accesso ai documenti amministrativi, rimette all'amministrazione ed al giudice la ponderazione comparativa tra il diritto alla riservatezza dei dati riguardanti la salute o la sfera sessuale e l'interesse sotteso alla domanda di accesso. E il bilanciamento degli opposti interessi, in tal caso, non va effettuato in astratto, bensì in concreto in modo tale da evitare il rischio di soluzioni generalizzanti fondate su di una mera comparazione gerarchica dei diritti in conflitto che, prescinde da specifiche circostanze di fatto relative alle singole fattispecie concrete. Cfr, fra le tante Cons di Stato sez VI n, 2542/2002, http://www.giustizia-amministrativa.it/webcds/ElencoSentenze.asp; Cons di Stato, sez V n. 6681/06, http://www.giustizia-amministrativa.it/webcds/ElencoSentenze.asp; Cons. di Stato sez IV n 2639 /2010, http://www.giustiziaamministrativa.it/DocumentiGA/Consiglio%20di%20Stato/Sezione%204/2008/20 0806217/Provvedimenti/201002639_11.XML cfr. anche http://www.commissioneaccesso.it/ giurisprudenza2010.aspx.

La valutazione sulla domanda di accesso o comunicazione deve tenere presente anche i principi di necessità, pertinenza e non eccedenza dai dati.

crescente rilevanza nelle reti telematiche, soprattutto in ambito medico. Questa si presenta sotto diversi punti di vista, come ad esempio:

- rispetto della riservatezza dei dati contro la possibilità di lettura ed uso non autorizzati;
- controllo delle autorizzazioni e dei mandati per l'introduzione o la modifica dei dati;
- protezione dei dati da perdite o modifiche accidentali (back – up)[286].

L'Autorità garante ha, inoltre, più volte ricordato che il trattamento dei dati personali nei sistemi di CCE locali deve rispettare pienamente le norme che disciplinano la protezione di tali dati, sia livello nazionale che sovranazionale.

Le cartelle elettroniche locali, infatti, costituiscono in ogni caso un documento sanitario regolato da specifiche disposizioni normative. Il trattamento dei dati utilizzati nell'ambito di tali iniziative è così regolato dal Codice in materia di protezione dei dati personali (cfr., in particolare, artt. 75 e ss. e art. 20 del Codice)

Tuttavia, il sistema di gestione della cartella clinica elettronica locale (inteso in senso stretto come programma che permette di registrare e gestire l'insieme di dati su un paziente) si colloca oggi in un contesto di evoluzione più vasto. La diffusione delle reti telematiche e degli standard di comunicazione sanitaria permette, infatti, di importare documentazione generata da autori diversi in località differenti.

Si assiste, perciò, allo sviluppo anche di fenomeni peculiari che necessitano per questo di una distinta disciplina. Fra questi rientra il cd "Fascicolo sanitario elettronico" (*Eletronic Health Record* o cartella clinica elettronica - Fse), un documento elettronico contenente i dati sanitari di ogni paziente - patologie, interventi chirurgici, esami clinici, farmaci ecc.

Il fascicolo sanitario elettronico rappresenta l'integrazione delle cartelle cliniche locali, generalmente attraverso uno strumento accessibile tramite web, e raccoglie la storia clinica di un paziente dalla nascita alla morte.

Il Fse è consultabile dal paziente e aggiornabile on line da medici, farmacisti, enti ospedalieri ecc. Al momento, in Italia è in via di

[286] A. Rossi Mori, F. Consorti, Dalla cartella clinica elettronica locale al fascicolo sanitario personale, consultabile su http://www.e-osiris.it/data/docs/it260_cartella%20clinica%20elettronica13.doc.

sperimentazione in alcune Regioni e dal 2004 è allo studio del Tavolo di lavoro permanente della Sanità Elettronica, ma presto potrebbe diventare il modo normale di raccolta delle informazioni in ambito sanitario.

Anche negli altri Paesi tecnologicamente avanzati è previsto di poter garantire ad ogni cittadino un fascicolo sanitario personale[287], in tempi relativamente brevi.

Oltre agli indubbi e sicuramente importanti vantaggi in termini di qualità, velocità ed efficienza dell'assistenza sanitaria, uno dei primi problemi imposto da questa nuova comunicazione, strutturata tramite un intermediario automatizzato, è l'interoperabilità tra applicazioni eterogenee.

Tutte le applicazioni coinvolte, infatti, devono essere in grado di dialogare tra loro e di gestire l'informazione in modo appropriato, per questo la standardizzazione nell'informatica sanitaria è oggetto di diverse iniziative sia livello europeo[288] che internazionale.

Inoltre, "la peculiarità della condivisione da parte di distinti soggetti delle informazioni sanitarie che documentano un insieme di eventi di rilevanza medica, occorsi a uno stesso individuo, giustifica la formulazione di particolari considerazioni rispetto alla gestione cartacea di analoghi documenti e alla più generale tematica dell'informatizzazione sanitaria"[289].

I maggiori rischi e le diverse modalità di lesione del diritto alla riservatezza, potenzialmente insiti nell'uso di questo documento elettronico, la necessità, quindi, di strumenti di tutela specifici rispetto a quelli elaborati per la cartella clinica cartacea nonché l'assenza di una disciplina normativa interna in merito hanno portato il Garante alla predisposizione di un quadro di regole e principi, attraverso le "Linee guida in tema di fascicolo sanitario elettronico e di dossier sanitario"[290].

---

[287] L'analisi di queste strategie è in corso come attività dell'Istituto Tecnologie Biomediche del CNR nell'ambito del progetto OSIRIS. Materiale preparatorio è disponibile nei siti www.e-osiris.it e www.prorec.it.

[288] Cfr la Raccomandazione della Commissione 2008/594/CE http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:190:0037:0043: IT:PDF ed il "Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche" del 15 febbraio 2007 del Gruppo di lavoro europeo, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_it.pdf, http://www.sanita.forumpa.it/_documenti/0/200/290/297/lesperienza42.html.

[289] "Linee guida in tema di fascicolo sanitario elettronico", Pubblicato in G.U. n. 71 del 26 marzo 2009 e consultabile all'indirizzo http://www.garanteprivacy.it/garante/doc.jsp?ID=1598313, sono state adottate in via definitiva, a seguito di consultazione pubblica, con deliberazione del 16 luglio 2009, G.U. n. 178 del 3 agosto 2009, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1634116.

[290] Vedi nota precedente.

La particolare delicatezza dell'argomento, però, ha spinto il Garante, prima dell'adozione definitiva, ad aprire una consultazione pubblica, chiusa il 31 maggio, al fine di raccogliere le osservazioni ed i commenti, "in particolare da parte di organismi e professionisti sanitari pubblici e privati, dei medici di medicina generale e dei pediatri di libera scelta, di organismi rappresentativi di operatori sanitari e di associazioni di pazienti interessati."[291].

Come precisato dalle linee guida, "si parla di dossier sanitario qualora tale strumento sia costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es. ospedale o clinica privata) al cui interno operino più professionisti[292]. Si intende, invece, per Fse il fascicolo formato con riferimento a dati sanitari originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale (es., azienda sanitaria, laboratorio clinico privato operanti nella medesima regione o area vasta). I dossier sanitari possono anche costituire, ad esempio, l'insieme di informazioni sanitarie detenute dai singoli titolari coinvolti in una iniziativa di Fse regionale".

Gli argomenti fondamentali trattati poi dalle suddette linee guida riguardano la gestione, condivisione e protezione dei dati sanitari, in particolare:

a) finalità del Fse e del dossier sanitario. Questi devono essere utilizzati e, quindi, costituiti solo per di finalità di prevenzione, diagnosi, cura e riabilitazione, "con esclusione di ogni altra finalità (in particolare, per le attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, che possono essere, peraltro, espletate in vari casi anche senza la disponibilità di dati personali), ferme restando eventuali esigenze in ambito penale."

b) Costituzione di Fse o di un dossier sanitario. Le linee guida indicano la facoltatività nell'adozione di tali strumenti, sia dal punto

[291] Cfr http://www.garanteprivacy.it/garante/doc.jsp?ID=1598846.

[292] Vedi la nota 2 delle Linee guida: "In tal senso, il *dossier* sanitario si distingue dalla cartella clinica, dalle schede individuali del medico di medicina generale/pediatra di libera scelta e da quelle eventualmente tenute da medici specialisti con riferimento ai pazienti in cura presso gli stessi, in quanto poste in essere da un singolo professionista in qualità di unico titolare del trattamento. Qualora tali schede siano integrate con quelle di altri professionisti si potrebbe configurare un Fse, laddove i professionisti agiscano in qualità di autonomi titolari, ovvero un *dossier* sanitario, laddove i singoli professionisti, agiscano all'interno della medesima struttura sanitaria unica titolare del trattamento.".

di vista del titolare del trattamento, che può, ma ad oggi non deve adottarli, sia da quello del paziente[293].

c) Accesso. L'accesso ai dati contenuti nel Fse deve essere predisposto attraverso modalità adeguate ed è consultabile dall'interessato, dal personale sanitario e per finalità esclusivamente mediche. Non vi possono accedere, invece, periti, compagnie di assicurazione e datori di lavoro.

d) Consenso informato e specifico. Il paziente deve poter scegliere in piena autonomia e consapevolezza se costituire o meno il Fse e se far inserire solo alcuni dati sanitari e non altri. Deve poi essere prevista la possibilità di "oscurare" la visibilità di alcuni dati clinici[294].

Tale consenso è distinto rispetto a quello prestato in materia di cura della salute ed è revocabile[295]. Il soggetto che non acconsenta alla costituzione deve poter usufruire ugualmente delle prestazioni del servizio sanitario nazionale.

e) Informativa comprensibile e dettagliata. Tale disposizione è volta a garantire che il consenso dell'interessato sia realmente autonomo e libero.

f) Limiti alla diffusione e al trasferimento all'estero dei dati. "I dati sanitari documentati nel Fse/dossier non devono essere in alcun modo diffusi. La circolazione indiscriminata delle informazioni idonee a rivelare lo stato di salute, infatti, è vietata espressamente dal Codice (artt. 22, comma 8 e 23, comma 5, del Codice). La violazione

[293] "Il trattamento dei dati personali effettuato mediante il Fse o il *dossier*, perseguendo le menzionate finalità di prevenzione, diagnosi, cura e riabilitazione, deve uniformarsi al principio di autodeterminazione (artt. 75 e ss. del Codice). All'interessato deve essere consentito di scegliere, in piena libertà, se far costituire o meno un Fse/*dossier* con le informazioni sanitarie che lo riguardano, garantendogli anche la possibilità che i dati sanitari restino disponibili solo al professionista o organismo sanitario che li ha redatti, senza la loro necessaria inclusione in tali strumenti." Linee Guida, http://www.garanteprivacy.it/garante/doc.jsp?ID=1634116#b.

[294] "L'oscuramento' dell'evento clinico (revocabile nel tempo) deve peraltro avvenire con modalità tali da garantire che, almeno in prima battuta, tutti (o alcuni) soggetti abilitati all'accesso non possano venire automaticamente (anche temporaneamente) a conoscenza del fatto che l'interessato ha effettuato tale scelta ("oscuramento dell'oscuramento")". Idem, cit.

[295] "In caso di revoca (liberamente manifestabile) del consenso, il Fse/*dossier* non deve essere ulteriormente implementato. I documenti sanitari presenti devono restare disponibili per l'organismo che li ha redatti (es. informazioni relative a un ricovero utilizzabili dalla struttura di degenza) e per eventuali conservazioni per obbligo di legge, ma non devono essere più condivisi da parte degli altri organismi o professionisti che curino l'interessato (art. 22, comma 5, del Codice).", Idem cit.

di tale divieto configura un trattamento illecito di dati personali sanzionato penalmente (art. 167 del Codice).”[296]

g) Misure di sicurezza. La delicatezza dei dati trattati in ambito sanitario richiede l’adozione di adeguate misure di sicurezza volta a ridurre al minimo i rischi di accesso abusivo, furto e smarrimento.

A livello comunitario[297], inoltre, con una Raccomandazione[298] la Commissione europea ha invitato gli Stati membri a “garantire l’efficace e totale rispetto del diritto fondamentale alla protezione dei dati personali nei sistemi interoperabili di sanità elettronica, in particolare nei sistemi di cartelle cliniche elettroniche, in conformità delle disposizioni comunitarie sulla protezione dei dati personali con particolare riferimento alle direttive 95/46/CE e 2002/58/CE”.

La Commissione ha ritenuto, poi, che il trattamento dei dati contenuti nella cartelle cliniche elettroniche debba esser soggetto alla disciplina particolare, relativa al trattamento delle informazioni di natura delicata.

Al riguardo, si ricorda che l’articolo 8 della Direttiva n. 95/46/CE vieta, in linea di principio, il trattamento dei dati relativi alla salute di natura delicata, prevedendo, tuttavia, alcune deroghe a questo divieto, in particolare se il trattamento è richiesto per determinati motivi di ordine medico o sanitario.

Inoltre, secondo quanto previsto dalla stessa Commissione, “gli Stati membri devono seguire gli orientamenti sui sistemi di cartelle cliniche elettroniche forniti dal gruppo di lavoro costituito in base all’articolo 29 della direttiva 95/46/CE”[299], nella definizione di un quadro giuridico “completo per i sistemi interoperabili di cartelle cliniche elettroniche, che deve riconoscere e tenere conto della natura delicata dei dati personali relativi alla salute e prevedere le garanzie specifiche e appropriate per

[296] “Anche il trasferimento all'estero dei dati sanitari documentati nel Fse/*dossier* per finalità di prevenzione, diagnosi e cura dell'interessato può avvenire esclusivamente con il suo consenso, salvo il caso in cui sia necessario per la salvaguardia della vita o della incolumità di un terzo (art. 43 del Codice). Non a caso, nell'ambito dei progetti esaminati, la necessità di comunicare all'estero informazioni sanitarie dell'interessato contenute in tali strumenti si verifica prevalentemente per consentire all'interessato di usufruire di cure mediche all'estero o per consultare un esperto straniero.”Idem, cit

[297] Si veda anche il “Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche” del Gruppo di lavoro europeo del 15 febbraio 2007, cit.. La Commissione ed il Gruppo di lavoro europeo usano il termine Cartelle Cliniche Elettroniche indicate, dal Garante italiano, invece, come Fascicolo Sanitario Elettronico, nelle linee guida citate.

[298] Raccomandazione 2008/594/CE citata.

[299] Cit.

tutelare il diritto fondamentale alla protezione dei dati personali dell'individuo interessato".

Al riguardo, la Raccomandazione ha previsto che tale quadro giuridico sia finalizzato a: 1) analizzare i diversi impatti delle varie modalità di conservazione dei dati personali, riguardanti la salute, sulla tutela degli stessi e definire le strutture organizzative dei sistemi di cartelle cliniche elettroniche, che riflettano al meglio le specifiche tecniche e le prassi utilizzate a livello locale, regionale e nazionale, considerando i rischi specifici per i diritti e le libertà degli interessati. 2) Garantire l'autodeterminazione del paziente permettendogli di decidere in piena libertà e autonomia. 3) Per quanto possibile e se lo sforzo è commisurato al grado di protezione voluto, si deve sfruttare la possibilità di ricorrere a pseudonimi o di mantenere l'anonimato delle persone. d) Bisogna valutare anticipatamente i rischi e gli impatti specifici delle singole applicazioni. e) Alcune categorie di dati, quali i dati genetici o psichiatrici, potrebbero dovere essere totalmente esclusi dal trattamento on line o, perlomeno, essere soggetti a controlli d'accesso particolarmente rigorosi. f) E' necessario stabilire che il trattamento dei dati personali nelle cartelle cliniche elettroniche e nei relativi sistemi deve essere richiesto ed effettuato esclusivamente da un professionista in campo sanitario soggetto al segreto professionale, sancito dalla legislazione nazionale, o da altra persona, comunque, tenuta ad un obbligo di segretezza equivalente. g) Si devono stabilire le condizioni alle quali persone diverse dal soggetto interessato possono accedere e trattare dati relativi alla salute contenuti nei sistemi di cartelle cliniche elettroniche, e per quali fini sanitari. h) Va garantito un consenso pieno ed informato e che le informazioni fornite ai diretti interessati utilizzino un linguaggio ed un formato di facile comprensione e siano comunicate in maniera adeguata a persone con particolari esigenze (ad esempio bambini o anziani). i) Devono essere previste misure particolari per impedire che i pazienti siano illecitamente indotti a comunicare i dati personali contenuti nelle cartelle cliniche elettroniche. j) E' necessario assicurare che qualsiasi trattamento — specialmente la custodia — di dati personali contenuti nelle cartelle cliniche elettroniche abbia luogo in paesi che applicano la Direttiva n. 95/46/CE o paesi provvisti di un adeguato livello di tutela dei dati personali. k) Vanno stabiliti

nel dettaglio i requisiti in materia di controlli per garantire il rispetto degli obblighi nella tutela dei dati. l) Deve essere garantita la riservatezza dei sistemi di cartelle cliniche elettroniche e prevedere le adeguate misure tecniche e organizzative, facendo anche in modo che i casi di violazione siano individuati con prontezza ed efficacia, con la previsione di adeguate misure o soluzioni per gestirli, informandone e coinvolgendo le persone interessate, le autorità di controllo nazionali per la tutela dei dati e altri soggetti competenti in materia.

La Commissione ha indicato, inoltre, le linee guida per le attività di monitoraggio e valutazione nonché di istruzione e sensibilizzazione dei diversi soggetti coinvolti dai pazienti, al personale sanitario, agli enti pubblici e privati.

Riguardo quest'ultimo aspetto, in questo settore, così come anche negli altri ambiti trattati dal presente lavoro, l'educazione alla tecnologia è una questione assolutamente di primo piano, sia ai fini della tutela della privacy sia nel discorso più generale dello sviluppo delle risorse tecnologiche.

Tornando al tema generale delle informazioni idonee a rivelare lo stato di salute trattate in formato digitale, un ultimo accenno va al progetto di "Fascicolo Welfare", contenuto nel Libro bianco sul futuro del modello sociale[300] del Ministero del lavoro, della salute e delle politiche sociali, presentato nel maggio 2009.

In questo Libro è stato proposto come uno degli strumenti essenziali del prossimo scenario globale il Fascicolo personale elettronico, "destinato a raccogliere le informazioni inerenti le varie fasi della vita, nonché gli interventi preventivi, curativi e riabilitativi e più in generale tutte le informazioni utili per l'integrazione sociale e la partecipazione attiva al mercato del lavoro".

Il documento, quindi, conterrebbe la storia sanitaria del cittadino, ma anche ogni informazione relativa alla sua condizione socio-lavorativa, assistenziale e previdenziale.

Il Libro ha specificato, poi, che "la costruzione del fascicolo, la sua implementazione nel tempo, l'utilizzo delle informazioni e la loro

[300] www.lavoro.gov.it/NR/rdonlyres/376B2AF8.../0/librobianco.pdf; V anche L. BOLOGNINI e G. FORGESCHI, La *next privacy nella sanità digitale italiana*, in L BOLOGNINI, D. FULCO, P. PAGANINI, Next Privacy, op. cit, pag. 219.

tracciabilità pongono una grande sfida di innovazione tecnologica, ma soprattutto di cambiamento culturale, di responsabilità del cittadino verso la propria salute e del medico nei processi decisionali e terapeutici".

"(…) Sul versante del lavoro il fascicolo elettronico deve essere finalizzato a raccogliere e trasmettere informazioni strategiche sui percorsi educativi, formativi, occupazionali e assistenziali, in modo da prevenire il bisogno e favorire un ottimale inserimento nel mercato del lavoro (…). Il fascicolo sarà peraltro liberamente accessibile anche a tutti i servizi competenti al lavoro che necessitano di informazioni collegate in una ottica integrata in quanto fondamentali per l'inclusione sociale e la occupabilità. Pensiamo a una banca dati che, nel connettere e rendere effettivamente fruibili servizi oggi frammentati (libretto formativo, conto corrente delle posizioni assicurative presso le diverse gestioni previdenziali, sequenza dei rapporti di lavoro, titolarità di un sussidio da disoccupazione o sospensione del lavoro, assegni familiari,ecc.) aiuti a ricomporre in un disegno unitario carriere e percorsi formativi.".

Bene, se come più volte segnalato, in tema di circolazione dei dati attraverso le nuove tecnologie, uno dei rischi più sentiti è proprio quello dell'aggregazione/composizione dei diversi dati, in grado di costruire di veri e propri identikit virtuali della persona, i rischi per la tutela della privacy (e non solo per questa), insiti in tale progetto di fascicolo omnicomprensivo, sono piuttosto evidenti.

La raccolta in un solo "luogo digitale" di così numerose informazioni personali, anche particolarmente sensibili, comporterebbe innanzitutto correre il rischio di creare un enorme *single point of failure*[301], ovvero di consentire l'acquisizione indebita di moltissime informazioni sensibili colpendo un unico centro. L'acquisizione indebita potrebbe avvenire anche attraverso un'inadeguata suddivisione delle competenze e delle accessibilità alle informazioni.

In secondo luogo, la formazione di identikit virtuali potrebbe esporre al rischio di discriminazioni sociali ed economiche, si pensi fra gli altri ai casi in cui il contenuto del fascicolo venga a conoscenza di un datore di lavoro,

[301] L. BOLOGNINI e G. FORGESCHI, *La next privacy nella sanità digitale italiana*, in L BOLOGNINI, D. FULCO, P. PAGANINI, Next Privacy, op cit, pag. 219.

di una compagnia di assicurazione, di una banca in una procedura di richiesta mutuo o finanziamento da parte del cittadino.

L'adozione di tale strumento renderebbe, pertanto, necessaria la predisposizione di specifiche misure di sicurezza per scongiurare la possibilità di trattamenti illeciti, eccedenti, non necessari o scorretti: ad esempio "la separazione delle fonti di dati in diversi e distinti database, collocati su server differenti, interrogabili in modalità protetta da un robot centrale che sarebbe in grado di comporre, a seconda dei richiedenti e del loro particolare profilo di autorizzazione, il Fascicolo Welfare di volta in volta utilizzabile"[302].

Rispetto alla finalità perseguita, infine, non bisogna dimenticare la necessità della valutazione preventiva sull'effettiva utilità del fascicolo omnicomprensivo alla luce dei principi di necessità e proporzionalità, previsti dal Codice in materia di protezione dei dati personali.

2.2. I referti on line

L'attività di refertazione in rete costituisce un'altra area di rilievo nello sviluppo dei sistemi informativi in ambito medico. Con referto medico si indica "la relazione scritta rilasciata dal medico sulle risultanze di indagini diagnostiche, fisiche o strumentali"[303], mentre il "reperto" è il risultato dell'esame clinico o strumentale effettuato: ad esempio la radiografia.

Il referto, quindi, rappresenta l'interpretazione che il medico dà dei reperti diagnostici.

Sulla refertazione on line, il Garante della privacy italiano ha osservato come la conoscibilità dei referti da parte del paziente avvenga generalmente realizzata attraverso due modalità: la ricezione del referto presso la casella di posta elettronica dell'interessato oppure il collegamento al sito internet della struttura sanitaria dove è stato eseguito l'esame clinico, al fine di scaricare direttamente da lì il referto e, nei casi possibili, anche il reperto. In quest'ultimo caso, che sembra essere il più utilizzato, al paziente viene

[302] L. BOLOGNINI e G. FORGESCHI, *La next privacy nella sanità digitale italiana*, in L BOLOGNINI, D. FULCO, P. PAGANINI, Next Privacy, op cit, pag. 220

[303] Così Vocabolario di italiano, Garzanti

generalmente fornito un nome utente ed una password, all'atto della prenotazione o dell'effettuazione dell'esame.[304]

Alcune volte questi servizi sono accompagnati dall'invio al cellulare del paziente di un sms. Il Garante ha osservato che in questi sms non si deve comunicare altro se non la disponibilità dei referti, evitando il "dettaglio della tipologia di accertamenti effettuati, del loro esito o delle credenziali di autenticazione assegnate all'interessato".

La stessa Autorità ha sottolineato poi come queste modalità di ritiro dei referti on line si aggiungano, ma non sostituiscano quelle tradizionali, rimanendo facoltativa la scelta di adottarle sia da parte della struttura sanitaria sia dei pazienti, che possono liberamente e senza alcun pregiudizio non aderirvi.

Inoltre, l'assistito dovrà dare il suo consenso in base ad un'informativa chiara e trasparente che illustri tutte le caratteristiche del servizio di "refertazione on line". Il consenso, inoltre, non è generale ma relativo alla singola attività di refertazione. Lo stesso vale per la decisione dell'interessato di inviare il referto al medico curante o al medico generale/pediatra.

Allo stesso modo, un archivio di referti digitali formato presso un unico titolare del trattamento (es. un professionista o una clinica) forma un dossier sanitario, per il quale è necessario un ulteriore autonomo consenso, distinto da quelli prestati per le diverse refertazioni.

Per fornire il servizio la strutture sanitarie pubbliche e private dovranno garantire elevate misure di sicurezza tecnologiche, specificate nelle linee guida: ad esempio, utilizzo di standard crittografici, sistemi di autenticazione, convalida degli indirizzi mail con verifica on line, uso di password per l'apertura dei file[305].

Il referto, infine, resterà a disposizione on line per un massimo di 45 giorni e dovrà essere accompagnato da un giudizio scritto e dalla

[304] Linee guida in tema di referti on line, deliberate in via definitiva il 19 novembre 2009, G.U. n. 288 dell'11 dicembre 2009, consultabili su http://www.garanteprivacy.it/garante/doc.jsp?ID=1679033. Le stesse erano state precedentemente adottate con deliberazione del 25 giugno 2009, n. 21, su cui, nella stessa data il Garante aveva aperto una consultazione pubblica- entrambe sono state pubblicate sul sito dell'Autorità e su G. Uff. n. 162 del 15 luglio 2009- che si è chiusa il 30 settembre 2009.

[305] Vedi punto 6. Misure di sicurezza e tempi di conservazione dei dati, in Linee Guida in tema di referti on line, cit.

disponibilità del medico a fornire ulteriori indicazioni su richiesta dell'interessato[306].

2.3. La telemedicina

La telemedicina è l'insieme di tecniche mediche ed informatiche che permettono la cura di un paziente a distanza o più in generale di fornire servizi sanitari a distanza[307]. Le tecniche telemediche di fatto favoriscono anche applicazioni di formazione distanza, nelle quali il medico remoto può specializzare e aggiornare medici o altri operatori sanitari attraverso tecniche di *e-learning.*

La telemedicina abbraccia, quindi, un'ampia varietà di servizi, quali la "telediagnosi", la "teleassistenza", il "teleconsulto" e il "telesoccorso" quando si fa riferimento a integrazione, monitoraggio e gestione di pazienti, ma anche come osservato la "teledidattica", che, oltre alle indubbie utilità nel contesto nazionale, può assumere una connotazione ancora più importante se utilizzata per la formazione di personale presente in aree geografiche disagiate.

Sempre in quest'ambito, si evidenzia una delle applicazioni più comuni nell'ambito della telemedicina: la cd. *second opinion*, la quale consiste nel fornire un'opinione clinica a distanza supportata da dati acquisiti ed inviati ad un medico remoto che li analizza e li referta, producendo di fatto una seconda valutazione clinica su un paziente.

---

[306] In merito ai dati sanitari on line, si evidenziano i provvedimenti del Garante: 7 ottobre 2009 [doc. web. 1664456] su dati sanitari sul sito del Comune e 17 settembre 2009 [doc. web. 1658335] sulla trasparenza della P.A. e i dati sanitari on line; 16 dicembre 2009 [doc. web. n 1689148]sui dati sanitari sui siti delle aziende .

Si segnala anche il recente via libera del Garante privacy alla possibilità per i cittadini di prenotare visite specialistiche, pagare il ticket e ritirare referti medici direttamente presso il proprio farmacista. Occorrono però rigorose misure a protezione dei dati personali.

E' questo il contenuto del parere favorevole dell'Autorità sullo schema di decreto del Ministero della salute relativo all'erogazione di nuovi servizi sanitari da parte delle farmacie. Senza doversi recare alla Asl o in ospedale si potrà utilizzare la postazione collegata al Cup presente nelle farmacie. Parere del 19 gennaio 2011, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1787887.

[307] G. PAPI e F. RICCI, *La Telemedicina*, consultabile su http://www.uniroma2.it/didattica/fam/deposito/Telemedicina.pdf; L. BOLOGNINI e G. FORGESCHI, *La next privacy nella sanità digitale italiana*, in L BOLOGNINI, D. FULCO, P. PAGANINI, Next Privacy, op cit, pag. 215 e ss.. Si veda anche la Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla telemedicina a beneficio dei pazienti, dei sistemi sanitari e della società, COM/2008/0689 def., consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0689:FIN:IT:HTML

Fra i altri servizi di telemedicina si segnala, poi, in particolare la menzionata teleassistenza o telemonitoraggio. Questo è un servizio di telemedicina il cui obiettivo è di sorvegliare le condizioni di salute dei pazienti a distanza. La raccolta dei dati può avvenire o automaticamente, tramite dispositivi di controllo personale della salute, oppure tramite la collaborazione attiva del paziente (ad esempio, inserendo in uno strumento basato sul web le misurazioni del peso o dei livelli glicemici quotidiani).

Una volta elaborati e condivisi con i professionisti della sanità competenti, i dati possono essere utilizzati per ottimizzare i protocolli di controllo e trattamento del paziente.

Casi di teleassistenza sono, per esempio, quelli relativi al monitoraggio degli astronauti durante le loro missioni, così come nel settore marittimo[308], nei quali vengono gestiti da terra gli eventuali problemi sanitari. Altri esempi di utilizzo delle tecnologie di elaborazione dati si riscontrano nello svolgimento di indagini epidemiologiche o nell'assistenza di soggetti con gravi deficit motori.

Molti sono poi i tentativi nazionali ed internazionali di applicare alla medicina le tecnologie informatiche e bioingegneristiche. Si veda, al riguardo, il "Progetto per l'integrazione e la promozione degli ospedali e centri di cura italiani nel mondo"[309] (IPOCM) del Ministero della Salute e di altri Ministeri competenti. La finalità del progetto è quella di promuovere, attraverso l'uso in via continuativa di un servizio di teleconsulto medico e di formazione a distanza, la crescita della qualità delle prestazioni sanitarie erogate dai Centri Sanitari Italiani nel Mondo alle popolazioni che vi si rivolgono, spesso considerate –in tali contesti- categorie deboli. Al progetto aderiscono Centri Sanitari Italiani nel Mondo (CSIM)[310] collocati in 24 Paesi e Centri Sanitari Nazionali di Riferimento (CSNR)[311] in Italia,

[308] Vedi ad esempio il progetto avviato dal 2009 da Telesal insieme a Costa Crociere e all'Ospedale Galliera di Genova. Si tratta di un servizio di telemedicina attivo 24 ore su 24 che impiegando un sistema satellitare a banda larga consente la copertura sanitaria in remoto di ben cinquemila persone, ovvero i 3.780 ospiti e un migliaio di membri di equipaggio della nave da crociera Concordia. Nel servizio di telemedicina è coinvolto anche il CIRM (Centro Internazionale Radio Medico), che ha un'esperienza di oltre 70 anni di assistenza remota in mare e che recentemente ha avviato un'altra similare sperimentazione con l'armatore Finaval e la società specializzata in telemedicina Telbios. http://www.cwi.it/approfondimenti/2008/11/20/telemedicina-marittima-lultima-frontiera-sono-le-crociere./

[309] http://www.ipocm.salute.gov.it/ipocm/pdOspedali.jsp?language=italiano&id=563&area=ipocm.

[310] http://www.ipocm.salute.gov.it/ipocm/sezOrganizzazione_osp.jsp?men=orga&language=italiano&id=217.

[311] http://www.ipocm.salute.gov.it/ipocm/sezOrganizzazione_osp.jsp?men=orga&id=216&.

questi ultimi rappresentati da Istituti di Ricovero e Cura a Carattere Scientifico e grandi Ospedali pubblici e privati.

Per quello che riguarda l'aspetto qui trattato della tutela della privacy è evidente come il trattamento dei dati personali, le archiviazioni elettroniche e i flussi di risultati in formato digitale siano elementi collegati e strettamente connessi con le prestazioni di telemedicina. Così come si evidenzia che l'utilizzo di alcune specifiche tecnologie, impiegate in questo settore consentano di monitorare le persone a distanza in ogni momento.

Le tecnologie utilizzate vanno dalle etichette RFID, di cui si parlerà più avanti, agli strumenti di telefonia e Internet mobile (in grado di trasferire immagini, suoni e vari reperti diagnostici), fino ai dispositivi di geolocalizzazione, capaci di trasmettere in tempo reale la situazione fisica di un individuo, ovunque si trovi; alcuni sistemi sono in grado persino di percepire improvvisi sbalzi gravitazionali, avvisando cosi di eventuali cadute.

Per questo è importante che anche in questo settore si coniughino le attenzioni del giurista, del medico e dell'ingegnere per far sì che lo sviluppo delle applicazioni tecnologiche avvenga in modo da non ledere i diritti dei pazienti, tra cui, appunto la tutela della riservatezza e della dignità della persona[312].

Si tratterà, quindi, di regolare nel modo migliore i flussi digitali e le basi dei dati, garantendo al soggetto la massima trasparenza sul trattamento, la non eccedenza, proporzionalità, necessità e correttezza dello stesso ed assicurando, nello stesso tempo, adeguate misure di sicurezza per proteggere i dati raccolti.

L'intervento, però, dovrà anche investire a monte la stessa progettazione degli apparecchi utilizzati. Il singolo apparecchio applicato al corpo o alla sfera personale del paziente rappresenta, infatti, un primo livello di potenziale violazione della privacy, così più le tecnologie saranno costruite sicure, meno saranno i rischi di trattamenti illeciti e non autorizzati[313].

language=italiano.

[312] Vedi Comunicato stampa Garante Privacy - 23 febbraio 2005, "Rasi: telemedicina in espansione, necessarie garanzie di privacy", in http://www.garanteprivacy.it/garante/doc.jsp?ID=1099868.

[313] Si tratta della Privacy by Design per la quale si rinvia al paragrafo 4.1.5; cfr. L. BOLOGNINI e G. FORGESCHI, *La next privacy nella sanità digitale italiana*, in L BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, op cit., pag 217.

Sarebbe, pertanto, auspicabile che anche tutti i dispositivi di telemedicina avessero come requisiti essenziali imposti i sistemi "intrinseci" di protezione dei dati personali, così come previsto dalla Direttiva n. 1999/5/CE del Parlamento e del Consiglio, per le apparecchiature radio e le apparecchiature terminali di telecomunicazione.

Sempre in materia di tutela della privacy, nell'ambito del servizio di teleconsulto asincrono del progetto italiano IPOCM, su richiamato, è stato specificato che "l'esigenza primaria stabilita ex lege è quella di assicurare ai cittadini italiani una generale forma di protezione dei dati personali (art. 4 D.lgs. n. 196/2003) ed identificativi, rispetto ad un possibile uso *contra legem*, in quei campi in cui il trattamento dei dati (art. 4 D.Lgs. 196/2003) è effettuato attraverso l'utilizzo dell'informatica e della telematica."

In questo servizio, infatti, si assiste al trasferimento di informazioni relative ad un determinato caso clinico, potenzialmente trattato presso il Centro Sanitario richiedente.

"In applicazione al dettato normativo, quindi, il trattamento dei dati sensibili (art. 4 D.lgs. 196/2003) è rimesso ai suddetti Centri Sanitari compilatori delle schede di richiesta di teleconsulto, che dovranno garantire, sulla scheda, il completo anonimato dei dati contenuti, compresi quelli identificativi della persona eventualmente presenti negli allegati. In riferimento a questi ultimi -radiogrammi, immagini di cartelle cliniche, tracciati elettrocardiografici, ecc- l'anonimato verrà assicurato attraverso oscuramenti, meccanici o manuali, dei dati identificativi (art. 4 D.Lgs. 196/2003) o di qualsiasi altro elemento idoneo all'individuazione del soggetto che genera il caso clinico."[314]

2.4. I dati genetici

I dati genetici sono una categoria particolare di dati riguardanti la salute, così, il Codice in materia di protezione dei dati personali (d.lgs. 196/2003), in linea con la precedente normativa, per questi ha previsto una disciplina differenziata rispetto alle regole dettate per la più generica categoria dei dati sensibili (art. 26). All'art. 90, il Decreto subordina il trattamento delle

[314] http://www.ipocm.salute.gov.it/ipocm/sezNormativa_osp.jsp?men=norm&id=218&language=italiano

informazioni genetiche, "da chiunque effettuato", ad una "autorizzazione rilasciata dal Garante sentito il Ministero della salute, che acquisisce a tal fine il parere del Consiglio superiore di sanità".

Ai sensi dell'Autorizzazione generale al trattamento dei dati genetici, adottata il 22 febbraio 2007[315], per dato genetico si intende il dato che, indipendentemente dalla tipologia, riguarda la costituzione genotipica di un individuo, ovvero i caratteri genetici trasmissibili nell'ambito di un gruppo di individui legati da vincolo di parentela, il cd. "gruppo biologico".

I dati genetici si distinguono da ogni altra informazione poiché il patrimonio genetico è un patrimonio strutturale, definito e coglie il soggetto nella sua unicità, ponendolo in relazione in equivoca con altri soggetti[316]. Lo studio del Dna consente, quindi, di raccogliere informazioni delicatissime e tale raccolta può avvenire anche con l'assoluta inconsapevolezza del soggetto: sono sufficienti, infatti, un bicchiere utilizzato, un fazzoletto di carta, un capello, un mozzicone di sigaretta, una goccia di sangue.

Per ciò i dati genetici sono considerati i più sensibili tra i dati personali e sono utilizzabili solo in casi eccezionali, per finalità specifiche e con adeguate autorizzazioni[317].

L'analisi giuridica delle questioni connesse all'uso di questi dati riflette una delle caratteristiche della società dell'informazione, cioè quella di ricercare bilanciamenti non sempre facili tra interessi individuali e sociali, tra sfera pubblica e privata, tra interessi individuali configgenti.

L'Autorizzazione generale del Garante, sopra richiamata, si è occupata appunto di disciplinare i soggetti autorizzati al trattamento, la finalità e le modalità del trattamento, l'informativa da rilasciare, il consenso dell'interessato, che nella normalità dei casi deve essere prestato previamente e per iscritto, le misure di sicurezza, la conservazione, comunicazione e diffusione dei dati.

---

[315] Consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1389918, prorogata fino al 31 dicembre 2009 e successivamente, con delibera del 24 giugno 2010 (Gazzetta Ufficiale n. 158 del 9 luglio 2010), prorogata fino al 31 dicembre 2010. In ultimo, con deliberazione del 23 dicembre 2010, l'autorizzazione generale è stata prorogata fino al 31 giugno 2011, G. U. n. 2 del 4 gennaio 2011, consultabile su http://www.garanteprivacy.it/ garante/doc.jsp?ID=1776159.

[316] S. RODOTà, *Tecnologia e diritti*, op. cit., pag 208.

[317] Idem, pag. 209.

Secondo quanto prescritto, possono essere trattati i dati genetici inerenti alle finalità indicate che non possano essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa: per ragioni di tutela della salute del soggetto interessato o di un terzo appartenente alla sua stessa linea genetica (in particolare con riferimento a patologie di natura genetica e con l'obiettivo di tutelarne l'identità genetica); a scopo di ricerca scientifica o statistica "finalizzata alla tutela della salute della collettività"; quando il trattamento sia richiesto in forza di investigazioni difensive o divenga indispensabile "per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti espressamente dalla normativa comunitaria, da leggi o da regolamenti in materia di previdenza e assistenza o in materia di igiene e sicurezza del lavoro o della popolazione".

Infine, il ricorso ai dati genetici è altresì autorizzato "per l'accertamento dei vincoli di consanguineità per il ricongiungimento familiare di cittadini di Stati non appartenenti all'Unione europea, apolidi e rifugiati"[318].

Nel settore lavorativo, la facoltà di avvalersi di test genetici è ammessa quando sia richiesto dalla normativa comunitaria, dalla legge o da norme regolamentari, per scopi di "prevenzione delle malattie professionali", di "riabilitazione degli stati di invalidità", nonché "in materia di previdenza e assistenza o in materia di igiene e sicurezza del lavoro o della popolazione, anche senza il consenso dell'interessato". In quest'ultimo caso, però, il trattamento deve avvenire nel rispetto delle prescrizioni, contenute nell'Autorizzazione generale al trattamento dei dati sensibili nei rapporti di lavoro[319], e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'art. 111 del D.lgs. n.196/03.

Al di fuori di queste ipotesi, il ricorso alle informazioni genetiche è espressamente dichiarato illecito dalla citata Autorizzazione, quando sia "volt[o] a determinare l'attitudine professionale di lavoratori o di candidati all'instaurazione di un rapporto di lavoro, anche se basata sul consenso dell'interessato".

[318] In merito cfr P. TORRETTA, *Privacy e nuove forma di discriminazione rispetto alla circolazione delle informazioni genetiche:sistemi giuridici di tutela a confronto*, op cit.

[319] Ora Autorizzazione n. 1/2008 al trattamento dei dati sensibili nei rapporti di lavoro, del 19 giugno 2008, in G.U. n. 169, del 21 luglio 2008 - suppl. ord. n. 175, consultabile su www.garanteprivacy.it/garante/doc.jsp?ID=1529374.

Inoltre, "i dati genetici non possono essere comunicati e i campioni biologici non possono essere messi a disposizione di terzi salvo che sia indispensabile per il perseguimento delle finalità indicate dalla presente autorizzazione".

Per quanto riguarda la materia assicurativa, invece, il Garante della privacy ha posto, in conformità con la legge[320], il divieto di basare su dati di natura genetica l'attività di contrattazione di una polizza assicurativa[321].

La particolare attenzione riservata ai dati genetici si spiega, come già evidenziato, con il ruolo che questi assumo sempre di più all'interno della società. Sono visibili a tutti, infatti, le potenzialità che il continuo progresso scientifico e tecnologico sviluppa in termini di diagnosi e di intervento genetico con finalità scientifiche e curative; questo condurrà a quella che è stata definita la "società postgenomica"[322], in cui al caso si sostituirà sempre di più un potere di scelta da parte dei soggetti.

Tuttavia, proprio perché l'informazione sulle proprie caratteristiche genetiche è anche un importante e delicato "fatto privato", sono particolarmente rilevanti le questioni che si pongono in merito al bilanciamento dei diversi diritti coinvolti nelle loro dimensioni applicative inedite - come il diritto alla salute, alla ricerca scientifica, alla privacy, alla dignità umana e alla non discriminazione - nonché tutte le problematiche sulle modalità con cui i dati genetici sono raccolti e gestiti. Argomenti questi che inevitabilmente travalicano i confini nazionali.

Perciò è importante che gli ordinamenti (tanto quelli nazionali, quanto quello internazionale e comunitario) adottino un chiaro indirizzo verso l'assicurazione che i dati personali in genere, ma in particolare quelli inerenti alla sfera naturale/biologica dei soggetti, possano essere oggetto di un impiego ad esclusivo vantaggio del singolo e della collettività[323].

---

320 Il sistema italiano riconosce alle imprese assicuratrici la possibilità di disporre delle sole informazioni sullo stato di salute attuale del contraente, il quale è tenuto, in virtù della normativa codicistica (artt. 1897-1898), a fornire al riguardo le notizie di cui è a conoscenza, con esclusione delle informazioni genetiche di carattere predittivo.

321 Vedi anche le osservazioni espresse dal Gruppo misto Comitato Nazionale di Bioetica - Comitato Nazionale per la Biosicurezza, le Biotecnologie e le Scienze della Vita nel testo Test genetici e assicurazioni, del 20 ottobre 2008, p. 17, consultabile in www.governo.it/bioetica/gruppo_misto/test_genetici_assicurazioni_1.pdf.

322 S. RODOTà, Tra diritto e società. Informazioni genetiche e tecniche di tutela, in Riv. crit. dir. Pri., 2000, p. 571.

323 Vedi P. TORRETTA, *Privacy e nuove forma di discriminazione rispetto alla circolazione delle informazioni genetiche:sistemi giuridici di tutela a confronto*, consultabile su www.associazionedeicostituzionalisti.it/dottrina/libertadiritti/Torretta.pdf

Come indicato nell'Autorizzazione generale italiana, l'opportunità di ricorrere a simili informazioni deve essere perciò guidata dal proposito di consentire una più efficace ed incisiva garanzia della libertà e consapevolezza di scelta, nell'ottica di migliorare la qualità della vita, oppure dalla necessità di tutelare preminenti esigenze collettive aventi rilevanza costituzionale[324]

Il modo di utilizzazione delle informazioni genetiche si espone, infatti, a notevoli e pericolose possibilità di abuso fino alla loro vera e propria commercializzazione. A tale proposito, si guardino anche altri interventi del Garante per la protezione dei dati personali[325], nonché, a livello sovranazionale, ad esempio, quelli del Gruppo Europeo sull'Etica nelle scienze e nelle Nuove Tecnologie[326], in merito alla commercializzazione di massa dei test genetici.

Si stanno moltiplicando le offerte via internet di test genetici relativi soprattutto all'accertamento di paternità, ma anche alla predisposizione a diverse malattie (cardiache, diabete, ecc.). La pubblicità diventa sempre più aggressiva e capillare, anche in Europa: ad esempio, in alcuni Paesi compare all'interno popolari catene di negozi, nelle stazioni di servizio, negli autogrill lungo le autostrade, in televisione[327]. Molto spesso questi siti non sono supportati da medici e specialisti.

Questo fenomeno, come spiega il Garante, "pone molti e gravi problemi etici, sociali e giuridici e tende a trasformare uno strumento eminentemente diagnostico in una merce alla stregua di ogni altra".

Un'altra problematica, strettamente connessa alle caratteristiche delle informazioni genetiche, riguarda la possibilità che in base ad essi si creino discriminazioni individuali e sociali[328]. Si pensi, ad esempio, al problema già

[324] Cfr. Corte cost. 135/2002, in Giur. cost., 2002, p. 1062 ss.

[325] www.garanteprivacy.it

[326] Dichiarazione del Gruppo europeo sull'etica nelle scienze e nelle nuove tecnologie in merito alla pubblicizzazione di test genetici via Internet, 24 febbraio 2003, consultabile su http://www.privacy.it/cetestgenetici20030224.html. Vedi anche il Documento di lavoro sui dati genetici, del Gruppo di lavoro sulla privacy, adottato il 17 marzo 2004, consultabile su http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp91_it.pdf.

[327] Dichiarazione del Gruppo europeo sull'etica nelle scienze e nelle nuove tecnologie, cit..

[328] Vedi P. TORRETTA, *Privacy e nuove forma di discriminazione rispetto alla circolazione delle informazioni genetiche:sistemi giuridici di tutela a confronto*, op cit.; D. NELKIN, *Informazione genetica: bioetica e legge*, in Riv. critica del diritto privato, 4/1994, p. 491, M. PETRONE, *Trattamento di dati genetici e tutela della persona*, in Fam. e dir., 8-9/2007, p. 853 ss.; C. CASONATO, *La discriminazione genetica: una nuova frontiera nei diritti dell'uomo?*, in Atti del XV Convegno AIDC, Messina–Taormina, 2001, p. 2 ss; L. CHIEFFI, *Ingegneria*

segnalato degli screenig genetici in ambito lavorativo e assicurativo, vietati a livello europeo[329] e negli Stati Uniti - *Genetic Information Non-Discrimination Act* (GINA)[330]. In Italia il divieto, come si è visto, è stato ribadito dall'Autorizzazione generale del Garante del 2007.

A proposito della potenzialità prognostica dei test genetici si evidenzia, inoltre, la tutela riconosciuta, sia a livello internazionale - comunitario sia a livello italiano, del diritto dell'interessato a non essere informato dei risultati degli esami genetici e delle loro conseguenze[331]: si pensi, ad esempio, al caso di malattie genetiche incurabili come la "Corea Huntington".

Tra i documenti sovranazionali in materia di dati genetici si ricorda la Dichiarazione dell'Associazione mondiale dei medici[332], la quale ha contenuto le prime enunciazioni etiche in materia di applicazioni mediche dirette a migliorare i metodi di prevenzione, di diagnosi e di terapia delle malattie che colpiscono l'individuo e si informa al criterio della prevalenza del "benessere del soggetto umano (...) sugli interessi della scienza e della società" (punto 6).

genetica e valori personalistici, in L. CHIEFFI (a cura di), Bioetica e diritti dell'uomo, Paravia – Mondadori,Torino, 2000.

329 Vedi Documento di lavoro sui dati genetici, cit.; articolo 21 della Carta dei diritti fondamentali dell'UE "è vietata qualsiasi forma di discriminazione fondata (…)sulle caratteristiche genetiche" e tale divieto è contenuto anche nella Convenzione del Consiglio d'Europa sui diritti umani e la biomedicina (articolo 11) e nella dichiarazione universale dell'UNESCO sul genoma umano e sui diritti umani (articolo 6).

330 Consultabile su http://www.genome.gov/24519851. "Un sistema di sicurezza sociale e sanitaria con una forte connotazione privatistica costituisce un terreno privilegiato di verifica degli effetti che la circolazione dei dati relativi al patrimonio genetico individuale è in grado di produrre - in particolare nel settore delle assicurazioni sanitarie e dei rapporti di lavoro - sulla egualitaria 'distribuzione' di fondamentali beni di sostegno e di sviluppo della vita umana" così P. TORRETTA, *Privacy e nuove forma di discriminazione rispetto alla circolazione delle informazioni genetiche:sistemi giuridici di tutela a confronto*, op cit. Ivi per approfondimenti sulle legislazione americana e su quella di alcuni paese europei. Vedi anche E. JORIO, *La riforma sanitaria di Barack H. Obama*, in Federalismi.it, n. 17/2009, p. 1 ss., consultabile su http:www.federalismi.it.

331 Ne parla esplicitamente la Convenzione sui diritti dell'uomo e la biomedicina, approvata dal Consiglio d'Europa nel 1997 e ratificata dall'Italia nel 2001: "Ogni persona ha diritto di conoscere tutte le informazioni raccolte sulla propria salute e tuttavia si deve rispettare la volontà di una persona di non essere informata"; per una panoramica generale sui test genetici, vedi B. DALLA PICCOLA, *I test genetici: panoramica generale*, consultabile su www.privacy.it/dallapiccola20020321.html e G. FERRANDO, *Profili giuridici dei test genetici e decisioni riproduttive*, consultabile su www.privacy.it/ferrando2002032.html. Vedi anche L. CHIEFFI, *Analisi genetica e tutela del diritto alla riservatezza. Il bilanciamento tra il diritto di conoscere e quello di ignorare le proprie informazioni biologiche*, consultabile su http://www.associazionedeicostituzionalisti.it/ dottrina/libertadiritti/Chieffi.pdf.

332 La dichiarazione, adottata nella diciottesima Assemblea Generale della *World Medical Association* (WMA), tenutasi nel giugno del 1964 ad Helsinki in Finlandia, è stata più volte oggetto di modifiche nelle successive Assemblee generali dalla WMA, da ultimo a Seoul, nell'ottobre del 2008, consultabile su http://aix-scientifics.it/it/_helsinki2008.html.

Successiva, poi, è stata la Convenzione di Oviedo sui diritto dell'uomo e della Biomedicina[333], adottata dal Consiglio d'Europa il 4 aprile 1997, la quale oltre a vietare espressamente ogni discriminazione basata sulle caratteristiche genetiche dell'individuo (art. 11), ha rafforzato tale divieto con una serie di cautele e limiti che riguardo ogni indagine predittiva, imperniata sulle caratteristiche genetiche: la necessità di ottenere il consenso informato di chi si sottopone a test genetici (artt. 5 e 16), frutto del riconoscimento del carattere riservato proprio di ogni informazione sanitaria (art. 10), e la delimitazione del campo di impiego di simili indagini ad esclusive finalità sanitarie o di ricerca medica (art. 12).

Alla Convenzione di Oviedo è stato aggiunto di recente un Protocollo[334] che, in ordine agli interventi di biomedicina sull'essere umano, ha affermato il rispetto della natura inviolabile della persona, espressa nella garanzia, "senza discriminazione", della dignità, identità e integrità di ciascun individuo (art. 1).

Inoltre, lo stesso ha prescritto l'obbligo di preservare il carattere "confidenziale" di "ogni informazione a carattere personale raccolta in occasione di una ricerca biomedica", in osservanza "delle regole relative alla protezione della vita privata" (art. 25).

Si evidenzia, poi, la tutela antidiscriminatoria fornita dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, la quale, pur non menzionando all'art. 14 il fattore genetico, si è fatta portatrice del principio di eguaglianza a fronte di "ogni (…) condizione" dell'esistenza umana, e, sulla base di tale ampio significato, la Corte di Strasburgo ha individuato nella citata disposizione un parametro per

333 http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=164&CM=1&CL=ITA. Sul tema, fra gli altri, vedi G. QUACQUARELLI, *La Convenzione sulla biomedicina del Consiglio d'Europa*, in Riv. dir. pubbl. e Scienza politica, 1997, p. 265 ss.; G. CATALDI, *La Convenzione del Consiglio d'Europa sui diritti dell'uomo e la biomedicina*, in L. CHIEFFI (a cura di), Bioetica e diritti dell'uomo, op. cit., p. 267 ss. e C. PICIOCCHI, *La Convenzione di Oviedo sui diritti dell'uomo e della biomedicina: verso una bioetica europea?*, in Diritto pubblico comparato ed europeo, 2001, III, p. 1301 ss.

334 Consiglio d'Europa, Protocollo addizionale alla Convenzione per la protezione dei diritti umani e la dignità dell'essere umano nelle applicazioni della biologia e della medicina riguardante la ricerca biomedica., Strasburgo, 30 giugno 2004, GU n. 190 Suppl.Ord. del 14/08/2004, consultabile in inglese su http://conventions.coe.int/Treaty/EN/Treaties/Html/195.htm. V anche il protocollo firmato a Parigi il 12 gennaio del 1998 sul Divieto di clonazione degli esseri umani, consultabile su http://www.privacy.it/convoviedo2%201998.html. Si veda anche le Raccomandazioni R(92)3 e 97(5), G. SANTANIELLO, C. FILIPPI, *Dati genetici, genoma e privacy*, in A. LOIODICE, G. SANTANIELLO (a cura di), La tutela della riservatezza, Trattato di diritto amministrativo diretto da G. Santaniello, Cedam, Padova, 2000, pp. 521-526 e P. TORRETTA, *Privacy e nuove forma di discriminazione rispetto alla circolazione delle informazioni genetiche:sistemi giuridici di tutela a confronto*, op cit.

rigettare ogni trattamento pregiudizievole al "patrimonio irretrattabile", in cui sono sintetizzati i valori di "libertà-dignità" dell'individuo[335], a prescindere dalle caratteristiche personali, sociali e fisiche dello stesso[336].

L'11 novembre del 1997, poi, è stata approvata dall'Unesco la Dichiarazione universale sul genoma umano e i diritti dell'uomo[337], anch'essa espressione del tentativo di individuare principi condivisi e regole capaci di guidare la comunità internazionale a fronteggiare le sfide legate allo sviluppo scientifico e tecnologico ed evitare, così, che le applicazioni della ricerca biomedica possano comportare effetti inaccettabili sulla libertà, la riservatezza e la dignità della persona umana[338].

Sulla stessa linea, infine, si è postala Dichiarazione internazionale sui dati genetici umani, la quale ha stabilito le regole per la raccolta, il trattamento, la conservazione e l'utilizzo dei dati genetici contenuti in campioni biologici prelevati da individui, e la successiva Dichiarazione Universale sulla Bioetica e i diritti umani, adottate entrambe dalla Conferenza Generale dell'Unesco, rispettivamente il 16 ottobre 2003 e il 19 ottobre 2005[339].

In ambito comunitario, già nel 1989, con una Risoluzione del Parlamento europeo sulle problematiche relative alla manipolazione genetica[340], ha trovato spazio il tema delle implicazioni sociali, economiche, ambientali, giuridiche e sanitarie connesse al settore delle biotecnologie (punto 1).

---

335 Cfr., per queste espressioni, F. MODUGNO, *I "nuovi diritti" nella Giurisprudenza costituzionale*, Giappichelli, Torino, 1995, p.. 107. Vedi anche E. STEFANINI, *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, Cedam, Padova, 2008, p. 90, che attribuisce, in particolare, all'art. 11 della Convenzione di Oviedo un ruolo di completamento delle garanzie già espresse dalla CEDU, "estendendo il campo di applicazione dell'art. 14 anche a forme di discriminazione su base genetica".

336 Così P. TORRETTA, *Privacy e nuove forma di discriminazione rispetto alla circolazione delle informazioni genetiche:sistemi giuridici di tutela a confronto*, op cit.

337 Dichiarazione universale dell'Unesco sul genoma umano e i diritti dell'uomo, consultabile su http://www.portaledibioetica.it/documenti/004081/004081.htm.

338Il bio-diritto e le questioni ad esso legate hanno, infatti, carattere transnazionale, risentendo inevitabilmente del generale fenomeno di globalizzazione e della caratteristica sostanziale del suo presupposto: il linguaggio scientifico e le conseguenze delle applicazioni pratiche della tecnologia in generale sono "intrinsecamente" de-territorializzate.

Notevole rilevanza assumono, quindi, in questo ambito l'analisi comparata e la circolazione dei modelli di disciplina e di tutela degli interessi coinvolti Sulla necessità "di una integrazione giuridica europea e internazionale" nel campo della bioetica, vedi, ad esempio, L. PALAZZANI, *Introduzione alla biogiuridica*, Giappichelli, Torino, 2002, p. 97.

339 Dichiarazione internazionale sui dati genetici umani, consultabile su http://portal.unesco.org/en/ev.phpURL_ID=17720&URL_DO=DO_TOPIC&URL_SECTION=201; html Dichiarazione Universale sulla Bioetica e i diritti umani, consultabile su http://portal.unesco.org/en/ev.phpURL_ID=31058&URL_DO=DO_TOPIC&URL_SECTION=201.html.

340 GUCE n. C 96/116 del 17 aprile 1989.

In una successiva Risoluzione del 1996, sulla tutela dei diritti umani e della dignità dell'essere umano in relazione alle applicazioni biologiche e mediche[341], il Parlamento europeo ha sancito il divieto di cedere i risultati di indagini genetiche ad altre persone o istituzioni (in particolare, compagnie assicuratrici e datori di lavoro), salvo in caso di richiesta da parte dell'autorità giudiziaria o qualora intervenga l'esplicito consenso dell'interessato (punto 6).

Nel 2004 sono state approvate le "25 raccomandazioni concernenti le implicazioni etiche, giuridiche e sociali dei test genetici"[342], elaborate dalla Commissione europea con l'ausilio di un gruppo di esperti cui è stata affidata un'analisi interdisciplinare del tema.

Non va dimenticata, inoltre, la già analizzata Direttiva n. 95/46/CE[343], il cui art. 8 ha inserito i dati sulla salute fra le informazioni che richiedono precauzioni ulteriori e aggiuntive rispetto alle normali cautele che circondano l'impiego delle notizie relative alla sfera della persona. Sotto questa prescrizione, sembrerebbe potersi annoverare anche la sub-categoria dei dati genetici[344].

Inoltre, come già indicato, nel 2000 e nel 2007 a Strasburgo, in una versione riveduta, è stata proclamata a Nizza la Carta dei diritti fondamentali dell'Unione europea[345], la quale, oltre a riconoscere quelli già consolidati, si è aperta ad una nuova "generazione" di diritti[346] che si

[341] In GUCE n. C 320 del 28 ottobre 1996. Sempre riguardo alla materia delle biotecnologie, anche se non strettamente connessa all'argomento affrontato in questa sede, si ricorda anche la Direttiva 98/44/CE che sancisce il divieto di brevettare le invenzioni legate alla materia vivente, le invenzioni sul corpo umano in tutte le fasi della sua formazione e del suo sviluppo (artt. 4 e 5) e quelle "contrarie all'ordine pubblico e al buon costume" (art. 6).

[342] In http://ec.europa.eu/research/conferences/2004/genetic/pdf/recommendations_it.pdf, in merito vedi S. GAINOTTI, A.G. SPAGNOLO, *Test genetici: a che punto siamo in Europa*, in Medicina e morale, 4, 2004, p. 737 ss.

[343] GUCE n. L 281 del 23 novembre 1995, cit. Gli stessi criteri sono poi ripresi anche dal Regolamento (CE) n. 45/200168 (artt. 4 e 5), GUCE n. L 8, del 12 gennaio 2001, cit.

[344] P. TORRETTA, *Privacy e nuove forma di discriminazione rispetto alla circolazione delle informazioni genetiche:sistemi giuridici di tutela a confronto*, op cit.

[345] Carta dei diritti fondamentali dell'Unione europea, GUCE n C 303/1, 14 dicembre 2007, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0001:0016:IT:PDF.

[346] Così R. MASTROIANNI, *La tutela dei diritti fondamentali tra diritto comunitario e Costituzioni nazionali*, Relazione al Convegno della Corte di Cassazione "La tutela dei diritti fondamentali tra Corte costituzionale, Corti europee e giudice nazionale", Roma 21 gennaio 2009, consultabile su Osservatorio sul rispetto dei diritti fondamentali in Europa, www.europeanrights.eu, 2009, p. 17.

accompagna all'evoluzione dei fenomeni scientifici e tecnologici, al fine di farne uno strumento al servizio della persona[347].

Oltre ciò, lo sviluppo tecnologico relativo trattamenti in ambito genetico ha portato in evidenza un altro fenomeno critico ai fini dell'utilizzo delle informazioni genetiche nel rispetto della privacy, della dignità e dell'uguaglianza, ovvero la creazione di banche dati del Dna.

L'art. 4.1 lett. p) del nuovo Codice in materia di protezione dei dati personali ha previsto una nozione generale di banca di dati, considerando tale qualsiasi complesso organizzato di dati personali, anche se ripartito in una o più unità dislocate in luoghi fisici differenti.

La genericità di tale definizione è idonea a comprendere in sé il riferimento a qualsiasi tipologia di dato, quindi, anche i dati genetici. A ciò consegue la possibilità di applicare anche alle banche di dati genetici sia le disposizioni generali del Codice sia quelle specifiche relative ai dati genetici, sia le disposizioni contenute nell'Autorizzazione generale al trattamento dei dati genetici [348]

Il Garante, inoltre, ha più volte ribadito la necessità che, con riferimento alla creazione di banche di dati genetici, non si prescinda mai dal rispetto dei principi di necessità, scopo (o finalità) e di proporzionalità.

In generale, le banche dati possono distinguersi in due tipi: le biobanche[349], finalizzate alla raccolta e conservazione di materiale biologico per fini medici e di ricerca e le banche di dati genetici per scopi giudiziari o di polizia.

Diverse possono essere le ragioni alla base della creazione di una biobanca, come ad esempio la necessità per i ricercatori di accedere a più campioni biologici per ragioni statistiche, scambiare campioni, effettuare più test sullo stesso campione o ripeterli in periodi diversi.

---

[347] P. TORRETTA, *Privacy e nuove forma di discriminazione rispetto alla circolazione delle informazioni genetiche:sistemi giuridici di tutela a confronto*, op cit.

[348] Cit. Dove, ad esempio, in ambito di misure di sicurezza si legge: "I dati genetici e i campioni biologici contenuti in elenchi, registri o banche di dati, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità, in modo da ridurre al minimo i rischi di conoscenza accidentale e di accesso abusivo o non autorizzato. Laddove gli elenchi, i registri o le banche di dati contengano anche dati riguardanti la genealogia o lo stato di salute degli interessati, le predette tecniche devono consentire, altresì, il trattamento disgiunto dei dati genetici e sanitari dagli altri dati personali che permettono di identificare direttamente le persone interessate".

[349] Vedi Parere Comitato nazionale di Bioetica del 9 giugno 2006, consultabile su http://www.governo.it/bioetica/testi/_Biobanche.pdf.

Sebbene siano un utile strumento per il miglioramento e lo sviluppo delle cure sanitarie, le biobanche destano notevoli preoccupazioni per quanto concerne la tutela della riservatezza. Gli interrogativi più rilevanti riguardano l'eventualità di un trattamento successivo di dati per finalità diverse da quelle che hanno condotto all'originaria raccolta, la durata di conservazione dei dati genetici, la previsione e adozione di adeguate misure di sicurezza.

E' accaduto (ed accade tuttora), infatti, che alcune banche di dati genetici siano state finalizzate al perseguimento di uno scopo di lucro. Queste banche raccolgono tessuti di donatori volontari e tessuti raccolti dagli ospedali, prima usati per ricerche mediche, per poi venderli ad istituti di ricerca. Alcuni enti di ricerca o commerciali possono richiedere licenze esclusive per accedere e utilizzare i dati raccolti.

E' quanto è avvenuto in Islanda[350], dove il Parlamento ha inizialmente autorizzato la creazione e l'utilizzo di una grande banca dati sanitaria centralizzata, destinata a raccogliere tutte le informazioni mediche sull'intera popolazione islandese.

Dopo l'approvazione di tale legge, il Parlamento ha venduto ad una società privata, la *DeCode Genetics*, il diritto di sfruttamento delle informazioni sanitarie relative alla popolazione dell'isola. L'intento dello Stato era quello di realizzare un profitto attraverso lo sfruttamento delle caratteristiche della popolazione islandese che, vissuta in un relativo isolamento (si è parlato a tale proposito di "isole genetiche"), dispone di un patrimonio genetico omogeneo che consente una ricerca mirata alla individuazione delle mutazioni genetiche all'origine di determinate malattie.

Le implicazioni in materia di tutela della riservatezza sono evidenti: appare, infatti, inadeguato l'anonimato delle informazioni, in quanto in

350. Per il caso Islanda vedi C. DI GIORGIO, *AAA in Islanda è in vendita il Dna*, 13 gennaio 1999, in http://www.repubblica.it/online/cultura_scienze/islanda/islanda/islanda.html; P. DE CAROLIS, *Schedatura del Dna, l'Islanda si ribella*, in Il Corriere della Sera 17 maggio 2004; D. BONACORSI, *In banca i geni d'Islanda*, Jekill giugno 1999, n.3, in http://www.sissa.it/ilas/jekyll/n03/articoli/articolo_2_etp.htm; *Guardatevi da chi vuol farvi del bene*, Newsletter 18-24 settembre 2000, in www.garanteprivacy.it (intervista pubblicata sulla Frankfurter Allgemeine Zeitung del 13 settembre 2000; *Test genetici. Conferenza internazionale a Roma*, Newsletter 18-24 marzo 2002, in *www.garanteprivacy.it* ; P.C. MARCHISIO, *La valle dei geni*, in La Stampa del 30 marzo 2005; F. PORCIANI, *Chi protegge il Dna degli italiani*, in Il Corriere della Sera, 23 maggio 2004, consultabile su http://archiviostorico.corriere.it/2004/maggio/23/Chi_protegge_Dna_degli_italiani_cs_0_040523156.shtml. Casi analoghi si sono verificati anche in Estonia, nelle isole di Tonga e in altre piccole comunità, tra cui anche alcune italiane.

piccole comunità i portatori di determinati difetti genetici sono più facilmente individuabili.

La vicenda della banca dati islandese ha visto anche l'intervento della Corte Suprema. Nel 2003 la Corte Suprema dell'Islanda ha concesso ad una donna la cancellazione dalla banca dei dati genetici del padre defunto, ponendo, però, a base del proprio ragionamento non la necessità di ottenere, nel caso specifico dai familiari del defunto, un consenso informato per l'utilizzo delle informazioni genetiche, bensì il fatto che l'interesse della figlia a mantenere la riservatezza dei dati del padre trovava giustificazione nel carattere condiviso ed ereditario di essi, ciò determinava quindi una lesione della privacy della donna[351].

Sempre in tema di bio banche si guardi ancora il dibattito nato intorno al cd. Progetto Genoma - che ha identificato tutti i geni dell'uomo - ed al recente progetto dell'Atlante del genoma del cancro (Tcga), il quale equivale ad almeno diecimila volte il precedente, in termini di Dna da sequenziare, di tempi e di costi. Il suo obiettivo, infatti, è quello di rivelare e descrivere in dettaglio tutte le alterazioni genetiche che possono trasformare una cellula sana in una maligna[352].

Il Progetto Genoma Umano ha interessato l'opinione pubblica per la sua importanza come progetto scientifico, ma ha anche suscitato interrogativi e preoccupazioni derivanti dalle prospettive riguardo alla tutela della dignità umana e, in generale, dei diritti fondamentali. In questo senso, mentre da un lato si è fatto riferimento ai benefici che possono derivare sul piano delle conoscenze fondamentali e delle possibilità diagnostiche e terapeutiche, dall'altro si sono sottolineate le considerevoli implicazioni di natura antropologica e sociale che quest'ultimo può avere[353].

Altrettanto di rilievo si mostrano, poi, alcune delle maggiori problematiche legate alla privacy e conseguenti alla formazione del secondo tipo di banche dati, ovvero quelle per finalità di polizia/giudiziarie.

---

[351] Sentenza 151/2003 della Corte Suprema dell'Islanda, consultabile su http://www.mannvernd.is/english/index.html.

[352] Cfr. R. DULBECCO, in *LeScienze*, aprile 2007; La mappa del genoma umano e i suoi dieci anni di storia http://www.liquidarea.com/2010/04/la-mappa-del-genoma-umano-e-i-suoi-dieci-anni-di-storia/.

[353] Vedi il parere del Il Comitato Nazionale per la Bioetica del 18 marzo 1994, consultabile su http://www.portaledibioetica.it/documenti/001740/001740.htm. I promotori del Progetto Genoma Umano hanno costituito al suo avvio nel 1990 una commissione speciale, la ELSI (Ethical, Legal and Social implications Project), http://www.genome.gov/page.cfm?pageID=10001618.

I principali vantaggi connessi alla costituzione di banche dati in questo settore riguardano, ad esempio, la possibilità di risolvere crimini più velocemente e con minori costi, identificare le persone attraverso l'analisi comparativa (*matching*) del DNA, con lo scopo di scoprire il colpevole, scagionare gli innocenti e/o mettere in relazione più crimini commessi dalla stessa persona, identificare persone scomparse o vittime ignote di disastri naturali o di altro tipo.

Senza dimenticare, inoltre, lo scambio di dati tra Forze di Polizia di Paesi diversi, nel cui ambito si rinviene, ad esempio, la possibilità di collegare diverse scene del crimine o rintracciare all'estero i colpevoli.

In questo contesto, il tema della creazione di banche dati genetiche si collega alla necessità, sempre più avvertita, di ricercare "un equilibrio fra due diritti fondamentali: la garanzia di sicurezza e il diritto alla libertà individuale e collettiva del cittadino"[354].

In Europa, già con la Risoluzione del Consiglio dell'Unione Europa del 9 giugno 1997 -sullo scambio di risultati di analisi del DNA (97/C 193/02)[355], gli Stati membri sono stati invitati a prevedere la costituzione di banche dati nazionali del DNA.

Attualmente gli Stati dotati di banche dati del Dna sono il Regno Unito (1995)[356], l'Olanda e l'Austria (1997), la Germania e la Francia (1998), la Finlandia, la Svezia e la Norvegia (1999-2000), la Svizzera, la Danimarca e il Belgio (2000), l'Ungheria e la Lettonia (2003)[357].

---

[354] Da una dichiarazione di F. Pizzetti apparsa sul *Sole 24 Ore* di Domenica 17 settembre 2006, in un articolo a firma di G. Romeo. Per l'analisi del rapporto fra privacy e sicurezza si rinvia al paragrafo 6.

[355] Consultabile su http://eurlex.europa.eu/Notice.do?mode=dbl&lng1=en,it&lang=&lng2=da,de,el,en,es,fi,fr,it,nl,pt,sv,&val=221446:cs&page=&hwords=null.

[356] Il tribunale di Strasburgo ha deliberato che la Gran Bretagna deve distruggere i dati relativi al Dna e alle impronte digitali di persone mai incriminate per alcun reato in quanto si tratta di una violazione dei diritti umani. Secondo le attuali norme, la polizia può raccogliere il Dna e le impronte di tutte le persone fermate e tenere queste informazioni nei loro archivi anche se l'individuo in questione viene in seguito assolto o se le accuse vengono ritirate. I giudici di Strasburgo hanno concluso che l'archiviazione dei dettagli di persone innocenti «non può essere considerata una pratica necessaria in una società democratica» e che potrebbe portare alla stigmatizzazione di questi individui. La sentenza chiude una battaglia legale durata sette anni tra il governo britannico e Michael Marper, un 45enne fermato per presunte molestie nei confronti della sua partner e un 19enne conosciuto soltanto come 'S', i quali - dopo che le accuse nei loro confronti erano state ritirate - avevano chiesto che i loro dettagli venissero cancellati dal database. S. and Marper vs United Kingdom, ECHR, NO. 30562/04 e 30566/04, 4.12.2008, consultabile su http://www.osservatoriocedu.it/Database/Sentenze/S%20E%20Marper%20C%20Regno%20Unito.pdf . Vedi anche L. SCAFFARDI, *Le banche dati genetiche per fini giudiziari e la libertà della persona*, in C. CASONATO C., PICIOCCHI, P. VERONESI (a cura di), Forum biodiritto 2008. La circolazione dei modelli nel biodiritto, Cedam, Padova, 2009 consultabile su http://www.forumcostituzionale.it/site/images/stories/pdf/documenti_forum/paper/0114_scaffardi.pdf.

[357] http://www.aifo-italia.it/all/0702-Ponti.pdf.

In generale, le normative hanno disciplinato l'impiego di database genetici per fini giudiziari in modo assai difforme, diversificandosi considerevolmente per le modalità di raccolta e gestione dei dati genetici.

Negli Stati Uniti, la legge federale che ha previsto l'istituzione e l'implementazione del *Combined DNA Index System* (CODIS) è del 1994[358].

In Italia, invece, dopo diversi disegni di legge[359], mai approvati, nel 2009, con la legge 30 giugno 2009, n. 85[360] è stato ratificato il Trattato di Prüm[361], chiamato anche "Schengen 2". Le legge ha previsto, tra le altre cose, l'istituzione, presso il Ministero dell'Interno - Dipartimento della Pubblica Sicurezza - della banca dati del Dna.

L'Accordo di Prüm (già siglato nel 2005 da Belgio, Germania, Francia, Lussemburgo, Olanda e Austria) ha lo scopo di rafforzare la cooperazione di polizia in materia di lotta al terrorismo, alla criminalità transfrontaliera e all'immigrazione clandestina.

L'Accordo contiene disposizioni concernenti lo scambio di dati riguardanti DNA e impronte digitali, lo scambio di informazioni su persone inquisite, sugli autoveicoli e i proprietari degli stessi, sul possibile utilizzo di *Sky Marshalls* - agenti in borghese che potranno confondersi tra i passeggeri degli aerei per contrastare possibili attentati terroristici o per il rimpatrio di criminali stranieri - da parte dei Paesi che intendano avvalersi di tale

---

358 Fin dal 1989 lo stato della Virginia ha iniziato ad utilizzare tali tipi di pratiche. Oggi tutti gli Stati americani raccolgono obbligatoriamente il DNA delle persone condannate per crimini sessuali mentre circa 40 di loro conservano il DNA di tutti i condannati per reati gravi. Vedi L. SCAFFARDI, *Le banche dati genetiche per fini giudiziari e la libertà della persona*, op cit.; S. AXELRAD, *Survey of State DNA Database Statutes*, in American Society of Law, Medicine, and Ethics, consultabile in http://www.aslme.org/dna_04/grid/guide.pdf.

359 Sul punto vedi A. CARLO, *La proiezione costituzionale della banca dati italiana del DNA per finalità di indagine criminale. Riflessioni a margine dei progetti di legge presentati nel corso della XV legislatura*, in C. CASONATO C. PICIOCCHI P. VERONESI (a cura di), Forum biodiritto 2008 La circolazione dei modelli nel biodiritto, op. cit., consultabile in versione provvisoria su http://www.jus.unitn.it/dsg/convegni/2008/ forum biodiritto/Papers/Carlo.pdf; Cfr anche la Segnalazione al Parlamento e al Governo sulla disciplina delle banche dati del Dna a fini di giustizia, del Garante in data 19 settembre 2007 ed il Parere dello stesso Garante del 17 ottobre 2007, consultabili rispettivamente su http://www.garanteprivacy.it/garante/doc.jsp?ID=1456163 e http://www.garanteprivacy.it/garante/doc.jsp?ID=1448799.

360 La legge 30 giugno 2009, n. 85, pubblicata in Gazzetta Ufficiale 13 luglio 2009, n. 160, consultabile su www.parlamento.it/parlam/leggi/09085l.htm.

361 consultabile su http://www.governo.it/GovernoInforma/Dossier/pacchetto_sicurezza/trattato_prum.pdf e http://www.camera.it/ 465?area=16&tema=16&Banca+dati+del+DNA; cfr anche C. SBAILO', *Trattato di Prüm, una rivoluzione silenziosa (finora)*, consultabile su http://www.forumcostituzionale.it/site/images/stories/pdf/documenti_forum/temi_attualita/guerra_terrorismo/0001_sbailo.pdf; Vedi anche il parere del Garante europeo dei dati personali, Parere 2007/C 169/02, in G.U.C.E., 21 luglio 2007, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007 :169:0002:0014:IT:PDF.

strumento, sui rimpatri congiunti, sulla falsificazione di documenti e sui pattugliamenti congiunti di frontiera.

Secondo la legge italiana di ratifica, la finalità dell'istituzione della banca dati e del laboratorio centrale è quella di facilitare l'identificazione degli autori di delitti, in particolare permettendo la comparazione dei profili del DNA di persone, già implicate in procedimenti penali, con gli analoghi profili ottenuti dalle tracce biologiche rinvenute sulla scena di un reato.

Sono stati poi modificati alcuni articoli del Codice di procedura penale. In tale ambito, tra l'altro, il legislatore ha dovuto fare i conti con una precedente sentenza della Corte costituzionale[362] che ha dichiarato l'illegittimità costituzionale dell'art. 224 del Codice di procedura penale, nella parte in cui consentiva al giudice, nel campo delle operazioni peritali, di disporre misure volte ad incidere sulla libertà personale dell'indagato, dell'imputato o terzi, al di fuori dei casi e dei modi previsti dalla legge.

Allo scopo di evitare promiscuità, molto pericolose sul piano della privacy, sono stati rigorosamente distinti tra loro i luoghi di: a) raccolta e confronto del DNA (banca dati nazionale); b) estrazione e conservazione dei campioni biologici dei profili (laboratorio centrale); c) estrazione dei profili provenienti dai referti (laboratori delle forze di polizia e specialisti).

Sia la banca dati sia il laboratorio nazionale sono sottoposti a controlli: della banca dati si occuperà il Garante per la protezione dei dati personali, mentre del laboratorio si occuperà il Comitato nazionale per la biosicurezza, la biotecnologia e le scienze della vita.

Sempre riguardo alla tutela dei dati personali, il provvedimento ha regolato il trattamento dei dati, l'accesso e la tracciabilità dei campioni e, in particolare, ha stabilito che i profili ed i relativi campioni non debbano contenere le informazioni che possono consentire la diretta identificazione del soggetto cui sono riferiti.

Per quanto concerne l'accesso alle banche dati, questo si configura di secondo livello: la polizia giudiziaria e la stessa autorità giudiziaria devono prima richiedere di eseguire il confronto e, solo se esso è positivo, potranno

[362] Sentenza n. 238/1996, relativa al noto caso della "Madonnina di Civitavecchia", consultabile su http://www.cortecostituzionale.it/informazione/rassegna_stampa/rassegnastampaquestionidecise/schedadec.asp?TrmD=&TrmDF=&TrmDD=&TrmM=&Comando=RIC&bVar=true&iPag=11511&iPagEl=; in merito vedi anche V. NAPOLEONI, *I prelievi ematici coattivi dopo la sentenza della Corte costituzionale n. 238/1996. Prospettive di intervento normativo*, consultabile su http://www.ipzs.it/Pubblicazioni_ministeri/Min_giustizia/Documenti_giustizia/pdf/1996/10_1996/10_1996_2069-2082.pdf.

essere autorizzate a conoscere il nominativo del soggetto cui appartiene il profilo.

Inoltre, è stata introdotta la necessità di identificare sempre e comunque l'operatore che ha consultato la banca dati, nonché di registrare ogni attività concernente i profili e i campioni.

Sono stati specificamente disciplinati, infine, i casi di cancellazione del profilo del DNA e di distruzione del relativo campione biologico e posti limiti temporali massimi – per la verità molto lunghi - per la conservazione nella banca dati nazionale del profilo del DNA (quarant'anni) e del campione biologico (venti anni).

Una delle problematiche sollevate dall'Accordo riguarda, proprio, l'aspetto della cancellazione dei dati e alla distruzione dei campioni. Nel corso dei lavori al Senato era stato proposto di aggiungere, all'art. 13, i riferimenti alla sentenza di non doversi procedere (art. 529 del c.p.p.), all'estinzione del reato (art. 531 c.p.p.), alla sentenza di non luogo a procedere (art. 425 c.p.p.) e al proscioglimento prima del dibattimento (art. 469 c.p.p.), ma il legislatore ha deciso in senso contrario, preferendo, secondo quanto asserito dal Relatore, varare rapidamente la norma[363].

Un'altra questione evidenzia, invece, la mancata previsione di garanzie per i membri appartenenti allo stesso gruppo biologico della persona a cui viene fatto il prelievo[364]. Ai familiari biologici non viene, infatti, richiesto alcun consenso e, addirittura, possono essere del tutto ignari della presenza del loro familiare all'interno della banca dati. Eppure, proprio per la strutturale condivisione dei dati genetici, in realtà anche questi risultano inseriti, seppur non ufficialmente, nella banca dati.

Restano, poi, in ogni caso, le preoccupazioni di ordine generale già espresse dai giudici della Corte europea dei diritti dell'uomo nella sentenza S. and Marper vs United Kingdom[365]. La formazione di database genetici a fini di indagini giudiziarie implica, infatti, come già osservato, un corretto bilanciamento fra gli interessi legati alla tempestiva repressione del crimine e i rischi legati a condotte invasive e discriminatorie nei confronti delle

363 Vedi C. SBAILO', *Trattato di Prüm, una rivoluzione silenziosa (finora),* op cit.

364 Vedi L. SCAFFARDI, *Le banche dati genetiche per fini giudiziari e la libertà della persona*, in C. CASONATO C. PICIOCCHI P. VERONESI (a cura di), Forum biodiritto 2008. La circolazione dei modelli nel biodiritto, op cit.

365 Sent. cit., vedi nota 356.

libertà fondamentali, della riservatezza e dignità della persona e del gruppo biologico ad essa legato .

Ci si trova in un ambito, in cui il più piccolo errore può produrre effetti gravi e anche talvolta irreversibili. Non solo eventuali abusi, ma anche interpretazioni emergenzialistiche della norma, infatti, possono aprire gravi *vulnera* nel sistema europeo di protezione dei diritti fondamentali.

Questa è una situazione, quindi, di fronte alla quale risulta quanto mai opportuno e necessario agire con molta prudenza.

Il trattamento dei dati genetici mostra come sia essenziale trovare una disciplina adeguata, avendo presente da un lato la continua evoluzione dell'innovazione scientifica e tecnica[366] e dall'altra che in questi settori, così delicati, vengono in considerazione diritti fondamentali, come la libertà personale, la dignità, l'uguaglianza, il diritto alla salute che possono dirsi rispettati e realizzati solo a fronte della esistenza di garanzie effettive e reali, riguardanti anche la riservatezza dei dati personali.

3. Privacy e E-government

Con il termine e-government si intende comunemente il processo di informatizzazione[367], della pubblica amministrazione, attraverso il quale è possibile trattare la documentazione e gestire i documenti stessi tramite strumenti digitali, grazie alle strutture proprie dell'ICT[368], allo solo scopo di rendere più snella ed efficiente l'attività degli enti locali e dell'amministrazione pubblica in generale, offrendo più servizi ai cittadini ed alle imprese, in un'ottica di trasparenza e fruibilità delle informazioni[369].

[366] "una disciplina elastica consente di evitare che leggi troppo rigide, pensate per l'eternità, vengano travolte dal continuo cambiamento determinato dall'innovazione scientifica e tecnologica; una disciplina leggera è quella che affronta soltanto questioni concrete, non sormontabili con strumenti diversi da quelli giuridici, e non pretende di dare risposte a preoccupazioni soltanto ideologiche o a generiche angosce sociali(..)" S. RODOTà, *Tecnologie e diritti*, cit, p. 139; cfr anche Cfr. S. RODOTà, *Diritto, scienza e tecnologia: modelli e scelte di regolamentazione*, in Riv. cri. dir. priv., a. XXII, n. 3, sett. 2004, p.372.

[367] Ovvero il processo attraverso il quale il mezzo informatico rende un oggetto materiale (es. documento), interoperabile e consultabile attraverso il computer.

[368] ICT è l'acronimo di *Information and Communication Technology*, con questo termine si intende, generalmente, la possibilità di trasmissione dati attraverso apparecchiature informatiche, anche se nell'ultimo periodo il termine è anche usato per indicare gran parte del mondo informatico.

[369] Cfr. S. STIZIA, *Informazione, nuove tecnologie e cambiamenti relazionali tra PA e cittadini*, in Diritto dell'Internet, Ipsoa, n.6/2006, p.615.

Negli ultimi anni il rapporto fra tecnologia e pubblica amministrazione ha visto il passaggio dall'introduzione dei primi strumenti informatici alla tele-amministrazione e digitalizzazione delle attività amministrative.

In particolare, le politiche di e-government, contenute nei recenti interventi legislativi e regolamentari, hanno mirato non solo alla realizzazione di un sistema informativo volto all'automazione delle procedure interne della pubblica amministrazione e all'erogazione dei diversi servizi ai cittadini ed alle imprese, ma anche all'erogazione di servizi ai singoli sistemi informatici delle amministrazioni, prevedendo la loro interconnessione[370].

Fra le diverse implicazioni della digitalizzazione della p.a. si evidenzia in particolare, per l'argomento trattato in questa sede, l'aumento esponenziale della raccolta di informazioni, nonché la notevole riduzione delle distanze, anche in termini temporali fra produzione, elaborazione e diffusione delle stesse. Perciò questo pone la necessità di contemperare tale sviluppo con le esigenze di tutela della riservatezza, della protezione dei dati personali e della sicurezza informatica in generale[371].

Da questo punto di vista, quindi, l'e-government si intreccia con la normativa in materia di privacy soprattutto quando viene richiesto alle pubbliche amministrazioni di rendere più fruibili ed accessibili i propri servizi, anche tramite strumenti che consentano al cittadino un'elevata autonomia ed interattività, come i siti o la posta elettronica.

3.1. Quadro normativo ed istituzionale

Le azioni italiane in materia di sviluppo dell'e-government (o amministrazione digitale) sono per la maggior parte attuazione a livello

[370] F. G. ANGELINI, *Pubblica amministrazione digitale, diritto di accesso e privacy*, in L BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, op cit, pag 260. Per poter realizzare un sistema informativo integrato ed unificato è necessario garantire che due o più applicazioni residenti in più sistemi, abbiano la possibilità di interoperare tra loro, svolgendo un'attività di comune interesse, sia a livello di condivisione e accesso reciproco dei dati, sia in prospettiva a livello di procedimentalizzazione elettronica delle varie fasi di competenza dei diversi enti, in un sistema di teleamministrazione. Così C. SILVESTRO, *E-government, e-governance, edemocracy*, in G. CASSANO (a cura di), Diritto delle nuove tecnologie informatiche e dell'Internet, IPSOA 2002, pag. 1279-1281.

[371] Cfr E-government: il punto dei Garanti europei, Newsletter del Garante per la protezione dei dati personali n. 174 del 9 - 15 giugno 2003, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=188992.

nazionale di indirizzi stabiliti in sede comunitaria, ciò ad ulteriore conferma che oggi quasi tutte le questioni assumono ormai una dimensione transfontaliera e globale[372].

Queste linee guida sono state efficacemente sintetizzate[373] in questi termini:

· creazione di un unico spazio europeo dell'informazione;

· innovazione e investimento nella ricerca;

· sviluppo e diffusione di servizi di amministrazione digitale per migliorare l'efficienza e l'efficacia della pubblica amministrazione;

· inclusione digitale, ovvero non lasciare indietro nessun cittadino rispetto alla fruizione di servizi di amministrazione digitale.

In Italia il recepimento di queste indicazioni si è mosso principalmente attraverso due direttrici: la definizione di un quadro normativo ed una serie di investimenti sia a livello di pubblica amministrazione centrale sia a livello regionale e degli enti locali, con la predisposizione di progetti cofinanziati.

Il nucleo dell'impianto normativo è costituito dal Codice dell'amministrazione digitale (CAD), emanato con D.lgs. 7 marzo 2005, n. 82 e sue successive integrazioni[374]. L'Italia è stata il primo paese a legiferare in materia di amministrazione digitale.

Il 19 febbraio 2010 il Consiglio dei Ministri, in virtù della delega contenuta nell'art. 33 della L. n. 69/2009, ha approvato il nuovo Codice dell'amministrazione digitale[375]. La tecnica utilizzata è stata quella della novella legislativa. Infatti, il successivo D.lgs. n. 235 del 30 dicembre 2010[376] non ha sostituito il vecchio testo con uno nuovo, ma vi ha apportato direttamente le modifiche, operando sui vecchi articoli. La

[372] Il Consiglio europeo con la Strategia di Lisbona, ratificata nel marzo del 2000, ha fissato, infatti, l'obiettivo "di fare dell'Unione Europea la più competitiva e dinamica economia della conoscenza del mondo" entro il 2010, sono seguiti poi i piani eEurope 2002, eEurope 2005 ed infine nella strategia i2010, vedi http://europa.eu/legislation_summaries/information_society/c11328_it.htm

[373] F. S. PROFITI, *Lo stato di attuazione dell'E-Goverment in Italia*, consultabile su http://www.cattolici-liberali.com/tocquevilleacton/pubblicazioni/focus/focus-paper20_ottobre08.pdf

[374] Consultabile su http://www.cnipa.gov.it/site/_files/Opuscolo%2013II.pdf.

[375] Consultabile su http://www.innovazionepa.gov.it/media/350095/nuovo_codice_della_amministrazione_digitale_cad.pdf; http://www.digitpa.gov.it/amministrazione_digitale.

[376] G.U. 10 gennaio 2011, n 6, consultabile su http://www.gazzettaufficiale.it/guridb/dispatcher?service=1&datagu=2011-010&task=dettaglio&numgu=6&redaz=011G0002&tmstp=1294735143548; Cfr anche P. RIDOLFI (a cura di), *Il nuovo Codice della Amministrazione Digitale*, Collana di Minigrafie, Tecnologia dei Processi Documentali, 2011 Fondazione Siav Academy - Edizione fuori commercio, consultabile sul sito http://www.digita-lex.it/pages/documents/ita/minigrafia7.pdf.

struttura del suddetto decreto legislativo presenta, quindi, una notevole complessità formale.

Le principali novità hanno riguardato: la riorganizzazione delle pubbliche amministrazioni - attraverso l'istituzione di un ufficio unico responsabile delle attività Ict - la razionalizzazione organizzativa e informatica dei procedimenti, l'introduzione del protocollo informatico e del fascicolo elettronico, la semplificazione dei rapporti con i cittadini e con le imprese - attraverso l'introduzione di forme di pagamenti informatici, lo scambio di dati tra imprese e Pa, la diffusione e l'uso della Pec, l'accesso ai servizi in rete, l'utilizzo della firma digitale - la dematerializzazione dei documenti e l'arricchimento dei contenuti dei siti istituzionali in termini di trasparenza.

Inoltre, è stata implementata la sicurezza dei dati attraverso la predisposizione, in caso di eventi disastrosi, di piani di emergenza per garantire la continuità operativa nella fornitura di servizi e lo scambio di dati tra Pa e cittadini.

Ancora, una volta operativo il nuovo CAD, il cittadino comunicherà una volta sola i propri dati alla PA centrale; sarà, poi, onere delle amministrazioni in possesso di tali dati assicurare, tramite convenzioni, l'accessibilità delle informazioni alle altre amministrazioni richiedenti.

In generale, comunque, sia il vecchio quanto il nuovo Codice, si inseriscono in un tessuto normativo volto alla costruzione di una nuova figura di pubblica amministrazione, maggiormente orientata verso i cittadini e *user friendly*[377].

Su questa linea, quindi, l'art. 3 commi 1, 1-bis e 1-ter. del CAD ha previsto il diritto del cittadino e delle imprese all'uso delle tecnologie informatiche come strumento per l'interazione con la Pubblica Amministrazione.

La normativa ha disciplinato poi gli strumenti utilizzati normalmente per operare con la pubblica amministrazione e necessari nell'ambito dell'amministrazione digitale: la firma elettronica, in sostituzione della firma autografa, la posta elettronica certificata, in sostituzione della comunicazione via fax o via raccomandata a/r, regole per i pagamenti

[377] E. BASSOLI, *E-Government e privacy*, consultabile in www.federalismi.it.

elettronici, lo sportello unico per le attività produttive anche in modalità telematica.

Infine, è stata promossa l'alfabetizzazione informatica dei cittadini, la formazione informatica dei dipendenti pubblici, lo scambio di informazioni tra pubbliche amministrazioni, attraverso modalità prettamente informatiche, basate sulle regole della Rete internazionale della pubblica amministrazione e del Sistema Pubblico di Connettività[378] (SPC).

Quest'ultimo, in particolare, è inteso come "insieme delle infrastrutture tecnologiche e delle regole tecniche per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione" necessarie per la realizzazione della "interoperabilità" - vale a dire dei servizi idonei a favorire lo scambio di dati e informazioni all'interno delle pubbliche amministrazioni e tra queste ed i cittadini - e della c.d. "cooperazione applicativa" che consente l'interazione tra i sistemi informatici delle pubbliche amministrazioni, permettendo così l'integrazione delle informazioni e dei procedimenti amministrativi[379].

Il Codice dell'amministrazione digitale, infatti, ha previsto l'accessibilità, da parte delle pubbliche amministrazioni, ai dati detenuti da altre amministrazioni secondo quello spirito di "leale cooperazione istituzionale" tra soggetti pubblici, già esplicitato nell'art. 22, comma 5° L. 241/90, definito ora, appunto, "cooperazione applicativa".

A tal fine, l'art. 14, comma 3 del CAD ha stabilito che lo Stato provveda alla creazione di organismi di cooperazione con le Regioni e le autonomie locali, promuovendo intese ed accordi tematici e territoriali, favorendo la collaborazione interregionale, incentivando la realizzazione di progetti a livello locale, in particolare mediante il trasferimento delle soluzioni tecniche ed organizzative, così ad auspicare programmaticamente

[378] F .S. PROFITI, *Lo stato di attuazione dell'E-Goverment in Italia,* op.cit. Il Sistema Pubblico di Connettività (SPC) è stato istituito con il Decreto Legislativo 28 febbraio 2005, n. 42 (pubblicato nella Gazzetta Ufficiale n. 73 del 30 marzo 2005), successivamente confluito nel CAD. Al sistema pubblico di connettività il d. lgs. 4 aprile 2006, n. 159 Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale, in G.U. n. 99 del 29 aprile 2006 – S.O. n. 105, ha dedicato l'intero Capo VIII "Sistema pubblico di connettività e rete internazionale della pubblica amministrazione".

[379] E. BASSOLI, *E-Government e privacy*, op. cit., pag. 11.

l'eliminazione del *digital divide*[380], tra amministrazioni di diversa dimensione e collocazione territoriale.

Anche per quanto concerne gli investimenti, di particolare rilievo è la forte collaborazione tra centro, Regioni ed Enti locali. Gli interventi sono stati articolati in due fasi distinte di attuazione (dette eGov fase I e eGov fase II).

L'art. 17del CAD, invece, ha previsto che le pubbliche amministrazioni centrali garantiscano l'attuazione delle linee strategiche per la riorganizzazione e digitalizzazione dell'amministrazione definite dal Governo, individuando un unico ufficio dirigenziale responsabile del coordinamento funzionale. A tale ufficio afferiscono i compiti relativi, tra gli altri, alla cooperazione e revisione della riorganizzazione dell'amministrazione, ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese, mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni, per la realizzazione e compartecipazione dei sistemi informativi cooperativi[381].

L'art. 68 ha previsto, ancora, che le pubbliche amministrazioni nella predisposizione o nell'acquisizione dei programmi informatici, adottino soluzioni informatiche che assicurino l'interoperabilità e la cooperazione applicativa e che consentano la rappresentazione dei dati e documenti in più formati, di cui almeno uno di tipo aperto, salvo che ricorrano peculiari ed eccezionali esigenze. E' stato così presupposto in generale lo scambio di dati fra pubbliche amministrazioni.

Peraltro, il Sistema pubblico di connettività, previsto dal CAD, deve anche garantire "la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione"[382]

I diversi progetti previsti del Codice sono stati, fino a poco tempo fa, coordinati e monitorati dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione[383] (CNIPA), organo che operava presso la

[380] *Digital divide*, è il termine tecnico utilizzato per definire le disuguaglianze nell'accesso e nell'utilizzo delle tecnologie.

[381] D.lgs. 82/2005, art.17, comma 1°, lett. *h*).

[382] Art. 73 comma 2 del CAD.

[383] http://www.cnipa.gov.it/.

Presidenza del Consiglio per l'attuazione delle politiche del Ministro per le riforme e le innovazioni nella PA e che unificava in sé due organismi preesistenti: l'Autorità per l'Informatica nella Pubblica Amministrazione (AIPA) ed il Centro tecnico per la Rete Unificata della Pubblica Amministrazione (RUPA). Il coinvolgimento di quest'organo in materia di amministrazioni digitale era sancito, a vari livelli di responsabilità e di indirizzo, direttamente nel CAD.

Il 29 dicembre 2010 è entrato in vigore il D.lgs. n. 177/2009, il quale ha previsto, tra l'altro, che il Centro nazionale per l'informatica nella Pubblica Amministrazione assuma ora il nome di DigitPA[384], con il relativo trasferimento delle funzioni.

Il DigitPA è un ente pubblico non economico che opera secondo le direttive e sotto la vigilanza del Ministro per la pubblica amministrazione e l'innovazione, con autonomia tecnica e funzionale, amministrativa, contabile, finanziaria e patrimoniale.

L'ente svolge funzioni di natura progettuale, tecnica, operativa e di coordinamento nei confronti della pubblica amministrazione centrale e di quelle locali[385]

A gennaio del 2009 è stato presentato dal Ministero per la Pubblica Amministrazione e l'Innovazione un piano d'azione denominato "Piano E-Government 2012"[386], finalizzato a colmare il divario nell'applicazione delle tecnologie nei servizi pubblici da parte dei cittadini italiani rispetto a quelli europei, attraverso l'applicazione del Codice dell'amministrazione digitale e avendo come punto di riferimento il piano d'azione europeo sull'e-goverment.

Il piano e-gov 2012 ha previsto, quindi, diverse iniziative volte ad allargare l'accessibilità on line della pubblica amministrazione, l'alfabetizzazione informatica dei cittadini, il potenziamento delle dotazioni e dei servizi nella scuola, nonché la "dematerializzazione"della pubblica amministrazione, ovvero la riduzione dello strumento cartaceo come supporto dei documenti e atti amministrativi[387].

[384] http://www.digitpa.gov.it/.

[385] Cfr http://www.digitpa.gov.it/digitpa/funzioni.

[386] http://www.e2012.gov.it/egov2012/index.php.

[387] Si legge, infatti nel piano che "una rilevazione effettuata dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA) nel 2004 su 61 amministrazioni centrali, ha evidenziato la

Altro obiettivo del piano è la riduzione del *digital divide* fra le diverse regioni italiane. Si legge, infatti, che "Infratel Italia ha già elaborato un piano d'intervento per il periodo 2008-2011 che punta ad una rapida e capillare diffusione della banda larga su tutto il territorio nazionale al fine di aggredire il digital divide infrastrutturale, pari approssimativamente a 4 milioni di abitanti, che si ridurrà del 50% circa al 2011 dopo due interventi nel Mezzogiorno e nel Centro Nord, per 400 milioni di euro circa."[388]

Inoltre, con la legge finanziaria del 2006 è stata istituita l'Agenzia per la diffusione delle tecnologie per l'innovazione[389], con lo scopo di integrare il sistema della ricerca con quello produttivo attraverso l'individuazione, valorizzazione e diffusione di nuove conoscenze, tecnologie, brevetti ed applicazioni industriali prodotti su scala nazionale ed internazionale.

Un altro elemento di rilievo nella struttura dell'e-government è rappresentato dal cd. "fascicolo informatico"[390], strumento cardine dell'intero iter procedimentale[391].

Secondo quanto disciplinato dal Codice, le regole per la costituzione e l'utilizzo del fascicolo sono conformi ai principi di una corretta gestione documentale ed alla disciplina della formazione, gestione, conservazione e trasmissione del documento informatico, ivi comprese le regole concernenti il protocollo informatico[392] ed il sistema pubblico di connettività. In ogni

produzione di 110 milioni di documenti, dalla quale discendono 160 milioni di registrazioni di protocollo e 147 milioni di documenti archiviati".

[388] http://www.e2012.gov.it/egov2012/index.php

[389] L'Agenzia per la diffusione delle tecnologie per l'innovazione, istituita con la legge finanziaria 2006, opera a livello nazionale ed è sottoposta ai poteri di indirizzo e vigilanza del Ministero per la Pubblica Amministrazione e l'Innovazione. Ha la finalità di accrescere la capacità competitiva delle piccole e medie imprese e dei distretti industriali attraverso la diffusione di nuove tecnologie e delle relative applicazioni industriali e di promuovere l'integrazione fra il sistema della ricerca e il sistema produttivo attraverso l'individuazione, la valorizzazione e la diffusione di nuove conoscenze, brevetti ed applicazioni industriali prodotti su scala nazionale e internazionale. http://www.aginnovazione.gov.it/it/index.html.

[390] Art 41 del Codice dell'amministrazione digitale.

[391] Relazione illustrativa al decreto legislativo 4 aprile 2006, n. 159 Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale, in G.U. n. 99 del 29 aprile 2006, S.O. n. 105.

[392] Con il D.P.R. 428/98 - in seguito abrogato dal D.P.R.. 445/2000 - il legislatore ha emanato il regolamento per la gestione del protocollo informatico che viene definito come "l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzate dalle amministrazioni per la gestione dei documenti". Con questo atto vengono fissati per la prima volta a livello normativo, i criteri generali. Sull'argomento Cfr E.BASSOLI, *E-Government e privacy*, op. cit., pag. 17 e ss.; http://www.cnipa.gov.it/site/it-it/Attivit%C3%A0/Protocollo_informatico/; http://www.interlex.it/pa/prot_norme.htm; P. RIDOLFI, *Amministrazione digitale. Compendio normativo*, Collana Minigrafie, Tecnologia dei processi documentali, Fondazione Siav Academy, 2010, consultabile sul sito www.digita-lex.it.

caso queste devono rispettare i criteri dell'interoperabilità e della cooperazione applicativa.

Inoltre, il fascicolo è consultabile e integrabile da parte di tutte le amministrazioni che intervengono nel procedimento[393], pur essendo nella sua costituzione e gestione curato dall'amministrazione titolare del procedimento.

Il fascicolo informatico, inoltre, deve avere i requisiti della facile reperibilità, corretta collocazione e collegabilità; in più è costituito e gestito in modo da consentire l'esercizio in via telematica dei diritti di cui alla L. n. 241 del 1990.

3.2. Tutela dei dati personali e sicurezza informatica nell'amministrazione digitale

Da quanto brevemente illustrato, emerge come la tematica del rapporto fra privacy ed e-government sia un argomento particolare in quanto non riguarda, semplicemente, il confronto fra cittadino e nuove tecnologie, ma anche quello del cittadino con la pubblica amministrazione presente in rete.

Infatti, questo generale processo di automazione e integrazione tecnologica nella p.a., sia nella sua organizzazione sia nei sui rapporti con i soggetti privati, pone inevitabilmente anche problematiche legate alla necessità di tutela del diritto alla privacy, in considerazione della enorme quantità di dati che entrerà, come osservato, nel patrimonio informativo delle diverse pubbliche amministrazioni, anche per il pregresso.

Non sono mancate al riguardo iniziative dell'Autorità garante, la quale ha segnalato diverse volte la necessità di una maggiore precisione e proporzionalità nell'identificazione della tipologia dei dati da inserire nei documenti, le persone che vi possono accedere e le garanzie da apprestare, soprattutto in relazione ai dati sanitari e biometrici.

Senza contare che comportamenti illeciti ed inidonee misure di sicurezza, oltre a ledere diritti, ostacolano la diffusione e l'uso delle tecnologie

[393] L'art. 41 del Codice prevede, quindi, una gestione flessibile del fascicolo da parte della pubblica amministrazione titolare, tuttavia il fascicolo può contenere aree riservate, cui hanno accesso solo la medesima P.A. o alcuni soggetti da essa individuati.

all'interno del tessuto economico e sociale, alimentando la diffidenza nei confronti delle stesse[394].

Il Codice dell'amministrazione digitale ha posto regole di garanzia in materia di tutela dei dati personali. L'art. 2 comma 5 ha sancito, in via generale, che le disposizioni del Codice "si applicano nel rispetto della disciplina rilevante in materia di trattamento dei dati personali e, in particolare, delle disposizioni del codice in materia di protezione dei dati personali approvato con decreto legislativo 30 giugno 2003, n. 196. I cittadini e le imprese hanno, comunque, diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato".

All'interno della normativa, ad esempio in tema di firme elettroniche e certificatori[395], l'art. 27 comma 2 lett. e ha previsto, poi, che il soggetto certificatore adotti "adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi private nei casi in cui il certificatore generi tali chiavi" .

Di seguito l'art. 32, comma 5, ha prescritto che "il certificatore raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dall'articolo 13 del decreto legislativo 30 giugno 2003, n. 196. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono".

In tema di segretezza della corrispondenza trasmessa per via telematica, l'art. 49 comma 1, ha imposto che "gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi

[394] cfr ad esempio quanto riportato su http://ansa.it/site/notizie/awnplus/internet/news/2009-05-12_112376716.html o http://www.helpconsumatori.it/news.php?id=23353.

[395] Ai sensi dell'art 1 lett. g del CAD il certificatore è "il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime"

trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche".

Così come è stato previsto il rispetto della normativa a tutela dei dati personali per quanto riguarda, in generale, il trattamento e la disponibilità dei dati da parte delle pubbliche amministrazioni, la sicurezza e l'accesso agli stessi[396].

Bisogna sottolineare, poi, che anche in quest'ambito un ruolo fondamentale è svolto proprio dalla sicurezza e, in questo settore in particolare, dalla sicurezza del sistema informatico della pubblica amministrazione.

Infatti, "qualunque informazione una Pubblica Amministrazione maneggi che sia riconducibile a cittadini identificati o identificabili– quindi pressoché tutte – deve essere protetta", così "quando noi parliamo di Pubbliche Amministrazioni in senso lato accade che la sicurezza sia oggi l'oggetto principale della privacy", perché " la privacy è la sicurezza, la sicurezza è la tutela dei dati dei cittadini"[397].

---

[396] Art. 50. Disponibilità dei dati delle pubbliche amministrazioni

1.I dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati; restano salvi i limiti alla conoscibilità dei dati previsti dalle leggi e dai regolamenti, le norme in materia di protezione dei dati personali ed il rispetto della normativa comunitaria in materia di riutilizzo delle informazioni del settore pubblico.

2.Qualunque dato trattato da una pubblica amministrazione, con le esclusioni di cui all'articolo 2, comma 6, salvi i casi previsti dall'articolo 24 della legge 7 agosto 1990, n. 241, e nel rispetto della normativa in materia di protezione dei dati personali, è reso accessibile e fruibile alle altre amministrazioni quando l'utilizzazione del dato sia necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente, senza oneri a carico di quest'ultima, salvo per la prestazione di elaborazioni aggiuntive; è fatto comunque salvo il disposto dell'articolo 43, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

3.Al fine di rendere possibile l'utilizzo in via telematica dei dati di una pubblica amministrazione da parte dei sistemi informatici di altre amministrazioni l'amministrazione titolare dei dati predispone, gestisce ed eroga i servizi informatici allo scopo necessari, secondo le regole tecniche del sistema pubblico di connettività di cui al presente decreto.

(Omissis)

Art. 52. Accesso telematico e riutilizzazione dei dati e documenti delle pubbliche amministrazioni

1. L'accesso telematico a dati, documenti e procedimenti è disciplinato dalle pubbliche amministrazioni secondo le disposizioni del presente codice e nel rispetto delle disposizioni di legge e di regolamento in materia di protezione dei dati personali, di accesso ai documenti amministrativi, di tutela del segreto e di divieto di divulgazione. I regolamenti che disciplinano l'esercizio del diritto di accesso sono pubblicati su siti pubblici accessibili per via telematica. (omissis).

[397] Così F. PIZZETTI, *Sicurezza, privacy, efficienza dei servizi: come conciliare i diritti per lo sviluppo di una moderna pubblica amministrazione*, Roma, 22 novembre 2007, consultabile su http://www.forumpa.it/convegni/sicurezzaprivacy/documenti/Pizzetti.pdf. Si vedano anche Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web, del 19 marzo 2011, Gazzetta

Sulla sicurezza dei dati, il Codice dell'amministrazione digitale ha prescritto all'art. 51 che:

"1. Con le regole tecniche adottate ai sensi dell'articolo 71 sono individuate le modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture.

1- bis (Omissis) [398]

2. I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.

2-bis. Le Amministrazioni hanno l'obbligo di aggiornare tempestivamente i dati nei propri archivi, non appena vengano a conoscenza dell'inesattezza degli stessi".

Per questo, nel 2002 è stato istituito un Comitato tecnico nazionale per la sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni, al fine di indirizzare e coordinare le diverse iniziative connesse con il Piano Nazionale della sicurezza Ict e definire gli standard di sicurezza nella pubblica amministrazione, mentre nel 2006 è stato redatto dal Gruppo di Lavoro, istituito presso il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (Cnipa), il documento: "Linee guida per la sicurezza ICT delle pubbliche amministrazioni"[399].

Su proposta del Comitato tecnico nazionale per la sicurezza informatica e delle telecomunicazioni nelle Pubbliche Amministrazioni, il Cnipa ha costituito al proprio interno, nel corso del 2004, l'unità di prevenzione e supporto alla PA centrale per le problematiche connesse alla gestione degli attacchi e degli incidenti informatici, denominato "GovCERT".

Ufficiale n. 64 del 19 marzo 2011, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1793203.

[398] Comma 1 – bis. DigitPA, ai fini dell'attuazione del comma 1:

a) raccorda le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici;

b) promuove intese con le analoghe strutture internazionali;

c) segnala al Ministro per la pubblica amministrazione e l'innovazione il mancato rispetto delle regole tecniche di cui al comma 1 da parte delle pubbliche amministrazioni.

[399] http://www.cnipa.gov.it/site/_files/Quaderno%20n%2023.pdf; http://www.cert_spc.it/index.php/download/govcert_/1469-normativa-e-linee-guida

Questa struttura, parallelamente ad analoghe realtà costituite in ambito europeo, ha operato dall'inizio del 2005 per supportare le pubbliche amministrazioni centrali nella prevenzione e gestione degli incidenti informatici, ponendosi come struttura di coordinamento dei gruppi per la prevenzione e la gestione degli incidenti informatici all'interno di ciascuna amministrazione centrale, a loro volta previsti dalla Direttiva sulla sicurezza ICT del 16 gennaio 2002 e denominati CERT-AM.

Una volta però diventato operativo il Sistema pubblico di connettività è stato necessario adeguarvi l'organizzazione della sicurezza informatica, così, ai sensi dell'art. 71 comma 1 bis del Codice delle amministrazione digitali è stato emanato il DPCM (1-4-2008)[400], contenente appunto le regole tecniche e di sicurezza per il funzionamento del SPC.

Il Decreto ha previsto che le funzioni di referente centrale nazionale per la prevenzione, il monitoraggio, il coordinamento informativo e l'analisi degli incidenti di sicurezza nel SPC siano svolte dal Computer Emergency Response Team del Sistema Pubblico di Connettività (CERT-SPC)[401], sul modello adottato a livello internazionale. La struttura, già operativa dall'inizio del 2008 all'interno del CNIPA (ora DigiPA), ha finito per sostituire, quindi, il precedente GovCert[402].

Le suddette Regole tecniche hanno previsto, poi, che ogni amministrazione centrale aderente all'SPC si doti di una Unità Locale di Sicurezza (ULS), cui è affidata sia la responsabilità di porre in atto tutte le fasi di prevenzione degli incidenti ICT, sia la gestione operativa degli eventuali incidenti informatici.

La soluzione organizzativa adottata per la prevenzione ed il contenimento delle conseguenze degli incidenti informatici, si caratterizza,

[400] Decreto del Presidente del Consiglio dei Ministri 1 aprile 2008 "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività previste dall'articolo 71, comma 1-bis del decreto legislativo 7 marzo 2005, n. 82, recante il «Codice dell'amministrazione digitale»." G.U. 21 giugno 2008, n. 144. Consultabile su http://www.cnipa.gov.it/HTML/RN_ICT_cron/spc_DPCM%201%20aprile%202008.pdf.

[401] http://www.cert-spc.it. Per le Regioni, le Regole Tecniche stabilisco la presenza di un CERT-SPC-R. A tal fine è operativo un gruppo di lavoro con le Regioni per definire, attraverso intese, le modalità partecipazione al sistema di sicurezza SPC, si veda ad esempio il Protocollo d'Intesa tra il CNIPA e la Regione Toscana, consultabile su http://www.e.toscana.it/e-toscana/resources/cms/documents/PI_cnipa_rt_8Lug2008.pdf .

[402] http://www2.cnipa.gov.it/site/_contentfiles/01380100/1380130_SEMINARIO_SICUREZZA_CNIPA.pdf.

quindi, con l'essere un modello basato su di una componente centrale e tante equivalenti componenti distribuite in ognuna delle amministrazioni.

3.3. La posta elettronica certificata (PEC) e le carte elettroniche

La posta elettronica certificata e le carte elettroniche rappresentano oggi alcuni degli strumenti dell'e-government maggiormente posti all'attenzione pubblica e che più coinvolgono la vita del singolo cittadino. Per questo di seguito se ne illustrano gli elementi fondamentali.

3.3.1. La posta elettronica certificata (PEC)

Per quanto riguarda la Posta Elettronica Certificata (PEC)[403], questa consiste in un tipo speciale di e-mail che consente di inviare/ricevere messaggi di testo e allegati, con lo stesso valore legale di una raccomandata con avviso di ricevimento, e rappresenta uno degli strumenti più importanti nel processo di digitalizzazione delle amministrazioni pubbliche.

La Pec, quindi, è fra le priorità del Piano di e-Government 2012, in cui è inserita come progetto "Casella elettronica certificata"[404].

Il CAD ha prescritto che le amministrazioni utilizzino la PEC per comunicare con i soggetti che hanno dichiarato il loro indirizzo, ai sensi della vigente normativa tecnica (Art. 6) e sono dotati di una casella PEC per ciascun registro di protocollo (Art. 47, c. 3). Inoltre, ha stabilito che le comunicazioni di documenti tra le PA sono valide, ai fini della verifica della provenienza, se trasmesse attraverso sistemi di PEC (Art. 47, c. 2).

In base all'art. 48 del CAD, la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante PEC o mediante altre soluzioni tecnologiche individuate

[403] D.P.R. n. 68/2005, consultabile su http://www.cnipa.gov.it/site/_files/DPR%2011%20febbraio%202005%20n.68.pdf, o nel nuovo sito http://www.digitpa.gov.it; per la normativa in generale si veda https://www.postacertificata.gov.it_/guida_utente/normativa-di-riferimento.dot e P. RIDOLFI, *Amministrazione digitale. Compendio Normativo*, op. cit., pag 78 e ss.; ai sensi dell'art 1 comma 1 v- bis, la per posta elettronica certificata si intende "sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi".

[404] Da aprile 2010 tutti i cittadini italiani - anche se residenti all'estero - hanno diritto gratuitamente a una casella di posta elettronica certificata (PEC) per effettuare via internet, con le pubbliche amministrazioni, comunicazioni di cui sia necessario certificare la spedizione, in sostituzione della raccomandata con ricevuta di ritorno. Cfr. http://www.digitpa.gov.it/pec/pec-al-cittadino; http://www.cnipa.gov.it/site/it-it/Attivit%C3%A0/Posta_Elettronica_Certificata__%28PEC%29/.

con decreto del Presidente del Consiglio dei Ministri, sentito DigitPA. Tale trasmissione equivale alla notificazione per mezzo della posta, salvo che la legge disponga diversamente.

Norme più recenti poi hanno esteso la portata della PEC, come strumento di scambio di documenti, dal solo ambito delle amministrazioni a quelli delle imprese, dei professionisti e dei cittadini[405].

Per quanto riguarda in particolare la tutela dei dati personali, specifica importanza svolge la sicurezza del servizio di trasmissione telematica di messaggi e documenti[406]. Oltre a quanto precedentemente osservato relativamente alla sicurezza del sistema pubblico di connettività, qui si evidenzia che l'utilizzo della posta elettronica certificata (pubblica) consente le sole comunicazioni tra cittadino e pubbliche Amministrazioni e viceversa e quello tra diverse pubbliche amministrazioni.

Riguardo alle caselle della pubblica amministrazione, la comunicazione è limitata alle pubbliche amministrazioni iscritte all'Indice P.A (IPA).

Tutte le connessioni, poi, sono realizzate tramite l'impiego di canali sicuri, basati sull'utilizzo dei protocolli di trasporto *Transport Layer Security* (TLS)/*Secure Sockets Layer* (SSL), che permettono la crittografia dei dati trasmessi in rete, mentre, per quanto riguarda i virus, vengono effettuati controlli sia nei messaggi in ingresso che in uscita.

Le configurazioni adottate, inoltre, sono tali per cui tutti i messaggi di PEC in cui è rilevata la presenza di virus sono consegnati al motore di PostaCertificat@ per essere trattati in conformità alla normativa vigente.

Ancora, le registrazioni (log), inerenti i messaggi scambiati, sono memorizzati su un registro riportante i dati significativi dell'operazione. I log dei messaggi sono conservati per 30 mesi a cura del gestore[407].

---

[405] La PEC per il cittadino (tecnicamente designata come CEC-PAC) può essere utilizzata solo per le comunicazioni con le Pubbliche Amministrazioni. Per comunicare con altri indirizzi PEC è necessario acquistare una casella PEC commerciale. Cfr http://www.digitpa.gov.it/pec/pec-al-cittadino e per la relativa normative cfr http://www.digitpa.gov.it/pec/normativa.

[406] Si vedano il Decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005 "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata." (G.U. 15 novembre 2005, n. 266), consultabile su http://www.digitpa.gov.it/sites/default/files/normativa/DM_2-nov-2005.pdf e l'Allegato al Decreto 2 novembre 2005. "Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata", il quale contiene tutte le regole e le specifiche tecniche per l'utilizzo della PEC, consultabile su http://www.digitpa.gov.it/sites/default/files/normativa/Pec_regole_tecniche_DM_2-nov-2005.pdf.

[407] Per quanto riguarda l'Indice P.A. (IPA), vedi http://www.indicepa.gov.it/, mentre per la sicurezza vedi https://www.postacertificata.gov.it/guida_utente/sicurezza.dot. Esempi di fattori critici per il trattamento dei dati personali possono rinvenirsi nel fatto che la conservazione per 30 mesi delle ricevute

Infine, per quanto riguarda la posta elettronica certificata, il Digitpa svolge sia un ruolo di vigilanza sui gestori del servizio che di supporto alle pubbliche amministrazioni per la sua introduzione nei procedimenti amministrativi[408].

Quanto alle garanzie per il trattamento dei dati personali da parte delle pubbliche amministrazioni, oltre a quelle generali già indicate [409] e previste dal CAD, l'art 46 dello stesso Codice ha prescritto in particolare che "al fine di garantire la riservatezza dei dati sensibili o giudiziari di cui all'articolo 4, comma 1, lettere d) ed e), del decreto legislativo 30 giugno 2003, n. 196, i documenti informatici trasmessi ad altre pubbliche amministrazioni per via telematica possono contenere soltanto le informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento e indispensabili per il perseguimento delle finalità per le quali sono acquisite".

Infine, l'art 47 comma 3 del CAD, ha previsto che l'utilizzo della posta elettronica per le comunicazioni fra l'amministrazione ed i propri dipendenti avvenga mediante la posta elettronica o altri strumenti informatici di comunicazione, "nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati", mentre, l'art. 49 del CAD ha assoggettato alla segretezza il contenuto della corrispondenza trasmessa per via telematica[410].

include anche l'intero messaggio e suoi eventuali allegati, anche se il gestore PEC è l'unico ad avere le credenziali per aprire "la busta di trasporto", non possono essere esclusi tentativi di accesso da parte di terzi dovuti a vulnerabilità del servizio del gestore o accessi abusi di soggetti dello stesso. Il gestore dovrà, quindi, munirsi di adeguate misure di sicurezza. Un altro nodo delicato relativo al trattamento dei dati personali è che la normativa non stabilisce dove vada a finire tutta la corrispondenza PEC e le informazioni in essa contenute dopo i trenta mesi.

[408] http://www.digitpa.gov.it/pec/ruolo-digitpa.

[409] Vedi ad es. artt. 50 e ss. del CAD, cit.

[410] Art 49. Segretezza della corrispondenza trasmessa per via telematica. 1. Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.

2.Agli effetti del presente codice, gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

3.3.2. Le carte elettroniche

Come già evidenziato anche la Carta di Identità Elettronica (CIE), la Carta Nazionale dei Servizi (CNS) ed il passaporto elettronico, sono strumenti ritenuti essenziali per l'innovazione tecnologica, per l'ammodernamento della pubblica amministrazione anche in termini di rapporto tra uffici pubblici e cittadini, e sono individuati nelle politiche di e-government come mezzi attraverso i quali gli utenti vengono riconosciuti in rete in modo certo, al fine di usufruire dei servizi erogati per via telematica dalle amministrazioni pubbliche[411].

In particolare, la carta d'identità elettronica (CIE)[412] è uno strumento di identificazione personale nonché di autenticazione per l'accesso ai servizi web erogati dalle Pubbliche Amministrazioni, come previsto dal Codice dell'amministrazione digitale (art.66). Le regole tecniche del nuovo

411 Cfr. P. CORSINI, E. ORBINI MICHELACCI, *Sostituire il documento cartaceo con il documento informatico, firmarlo e trasmetterlo in rete*, in "Diritto dell'Internet", Ipsoa, n. 3/2006, p. 311; P. RIDOLFI, *Amministrazione digitale. Compendio normativo*, cit. pag 63 e ss.

412 La carta d'identità elettronica è una *smart card* che integra nel supporto in policarbonato una banda ottica e un microprocessore. Più specificamente, i dati del titolare, compresa la foto, sono impressi in modo visibile sia sul supporto fisico, per l'identificazione "a vista", che sulla banda ottica e poi memorizzati informaticamente sul *microchip* e ancora sulla banda ottica. Per la normativa di riferimento cfr http://www.cnipa.gov.it/site/it-it/Normativa/Raccolta_normativa_ICT/Carta_d%E2%80%99identit%C3%A0_elettronica_e_carta_nazionale_dei_servizi/. Ai sensi dell'art. 1, comma 1 let c del Cad, per carta d'identità elettronica si intende "il documento d'identità munito di elementi per l'identificazione fisica del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare"

Sintomatico di come l'e-governement in Italia stenti ancora a decollare e presenti ancora deficienze e lacune è la vicenda legata alla proroga di validità della carta elettronica. Da quando , infatti, è stata prevista la proroga di 10 anni del documento di identità, per i possessori della CIE, la suddetta proroga è consistita, fino a poco tempo fa, in un documento cartaceo da esibire insieme a quello elettronico. Se non che tale documento non era riconosciuto da alcuni paesi stranieri, con grave disagio per il cittadino, magari fermato in quei paesi. La pezza messa dal governo a tale "inconveniente" è ancora più indicativa: infatti, con la circolare n.27 del 4-12-2009 (consultabile su http://www.servizidemografici.interno.it/sitoCNSD/documentazioneRicerca.do?metodo=dettaglioDocumento&servizio=documentazione&ID_DOCUMENTO=1129&codiceFunzione=CR&codiceSettore=AN), visto l'avvicinarsi delle festività natalizie, si invitavano gli addetti alla pubblica sicurezza di "volere nuovamente sensibilizzare i Sindaci, che avranno cura di sensibilizzare i cittadini, che intendano recarsi in viaggio nei Paesi indicati, di dotarsi di altro idoneo documento di viaggio" . Preso atto della figuraccia interna ed internazionale fatta, il Ministero dell'Interno ha emanato il 28 luglio una nuova circolare, la n 23 (consultabile http://www.servizidemografici.interno.it/sitoCNSD/ricercaNotizie.do?metodo=dettaglioNotizia &servizio=notizie&codiceFunzione=NT&ID_NOTIZIA=1218#), in cui si legge "Pertanto – in relazione ai quesiti pervenuti e sentito il Ministero degli Affari Esteri – attesa la particolare circostanza della inutilizzabilità per l'espatrio del documento d'identità prorogato con le modalità di cui sopra, si ritiene che si possa procedere alla sostituzione della carta d'identità da prorogare o già prorogata, seppur valida, con una nuova carta d'identità la cui validità decennale decorrerà dalla data del rilascio" ovviamente a spese del cittadino. Così, mentre a chi è in possesso della carta d'identità cartacea è sufficiente un semplice timbro, il fortunato in possesso del documento elettronico (decisamente in fase di sperimentazione) dovrà richiederne una nuova a sue spese. E' chiaro che una così la difettosa applicazione di strumenti di e-government non giova alla conquista della fiducia del cittadino nei confronti della p.a., digitale o meno che sia.

documento di riconoscimento personale, che dovrebbe debuttare ufficialmente nel 2011, sono state indicate nel Decreto Interministeriale dell'8 novembre 2007[413].

La carta contiene tutti i dati identificativi e le informazioni ufficiali relative alla persona e funzionerà anche come carta di servizi[414].

Oltre ai dati identificativi personali, ai sensi dell' art 66, comma 4 del Codice dell'amministrazione digitale, la carta d'identità elettronica può contenere, "a richiesta dell'interessato, ove si tratti di dati sensibili: a. l'indicazione del gruppo sanguigno; b. le opzioni di carattere sanitario previste dalla legge; c. i dati biometrici indicati col decreto di cui al comma 1, con esclusione, in ogni caso, del DNA; d. tutti gli altri dati utili al fine di razionalizzare e semplificare l'azione amministrativa e i servizi resi al cittadino, anche per mezzo dei portali, nel rispetto della normativa in materia di riservatezza; le procedure informatiche e le informazioni che possono o debbono essere conosciute dalla pubblica amministrazione e da altri soggetti, occorrenti per la firma elettronica.

L'introduzione all'interno della carta d'identità elettronica, per fini di semplificazione amministrativa, di altri dati diversi da quelli anagrafici e non strettamente necessari per la funzione di identificazione personale, ha posto, già al suo affacciarsi nel panorama legislativo, diverse questioni in ordine alla tutela della riservatezza dei cittadini.

La quantità di dati, anche sensibili, raccolta su ogni cittadino rischia di diventare in vero e proprio archivio, il cui utilizzo illegittimo potrebbe creare non pochi problemi. Già in riferimento alla Carta dei Servizi, il Garante espresse la necessità di particolari cautele e regole che evitassero la formazione di banche dati omnicomprensive, così come la raccolta e l'uso

[413] G.U. 9 novembre 2007 n. 229, S. O n. 261, consultabile su http://www.cnipa.gov.it/HTML/RN_ICT_cron/08/agg05/ ci_20071108_DM.pdf.

[414] Art 66, comma 8-bis del CAD: "Fino al 31 dicembre 2011, la carta nazionale dei servizi e le altre carte elettroniche ad essa conformi possono essere rilasciate anche ai titolari di carta di identità elettronica.". La Carta Nazionale dei Servizi è una *smart card* provvista esclusivamente del microchip (su un supporto fisico che non è necessariamente in policarbonato). Contrariamente alla CIE non si tratta in questo caso di un documento per l'identificazione a vista ma di uno strumento di autenticazione in rete che consente l'accesso ai servizi della P.A. resi disponibili per via telematica. La CNS è regolamentata ai sensi del decreto del Presidente della Repubblica 2 marzo 2004, n. 117 (G.U. 6 maggio 2004, n. 105) che ne stabilisce le modalità d'uso e di diffusione. La completa corrispondenza informatica tra CNS e CIE assicurerà l'interoperabilità tra le due carte e la continuità di servizi all'utente che passi della Carta Nazionale dei Servizi alla Carta d'Identità Elettronica. Cfr E.BASSOLI, *E-Government e privacy*, op. cit., pag. 20.

di dati personali in violazione dei principi di necessità, pertinenza e finalità[415].

Per quanto riguarda le regole tecniche e la sicurezza, l'art 8 del DPCM 22 ottobre 1999, n. 437[416] ha stabilito che sono dettate con decreto del Ministero dell'interno[417] le regole tecniche e di sicurezza, relative alle tecnologie ed ai materiali utilizzati per la produzione delle carte d'identità elettroniche, alle modalità di compilazione, rilascio, aggiornamento e rinnovo dei documenti e per garantire l'integrità, l'accessibilità e la riservatezza delle informazioni contenute nel documento.

Lo stesso articolo 8 ha previsto, poi, che le suddette regole tecniche e di sicurezza devono essere adeguate all'evoluzione delle conoscenze scientifiche e tecnologiche con cadenza almeno biennale.

Altre questione, legata all'inserimento di ulteriori dati all'interno della carte d'identità e del suo futuro uso come carte dei servizi delle pubbliche amministrazioni, è quella del cd. codice d'identificazione unico.

In molti paesi esiste già un identificatore unico utilizzato dai cittadini per i contatti con la pubblica amministrazione. Può trattarsi di un identificatore settoriale, come il codice fiscale italiano, oppure di un numero unico nazionale, come accade in Svezia e Finlandia[418].

---

[415] Si veda il parere del Garante al Ministero per l'innovazione tecnologica del 2003, di cui un sunto è contenuto nella newsletter del Garante n. 177 del 7 - 13 luglio 2003, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID =246147; quanto osservato da G. BUTTARELLI nel 2002 al Convegno: "Carta di identità elettronica e firma digitale: dalla sperimentazione ai servizi": " << Si tratta di dati, questi ultimi - ha precisato il Segretario generale - che in realtà aprono una serie di questioni riguardanti da un lato la loro effettiva utilità nell'essere inseriti nella carta di identità elettronica e la loro successiva utilità da parte di terzi, siano essi enti pubblici o strutture private e, dall'altro, gli aspetti tecnici su come effettivamente raccoglierli ed inserirli >>. Altri aspetti delicati derivano dal modo con cui sono registrati e accessibili, dalle tecnologie e dalle finalità prescelte (…) << L'Autorità garante - ha proseguito Buttarelli - ha perciò il compito istituzionale di richiamare l'attenzione nelle sedi istituzionali nazionali e negli organismi internazionali competenti sulla questione, in modo tale che la carta di identità elettronica possa garantire adeguate certezze riguardo alla protezione dei dati personali >>", cfr http://www.garanteprivacy.it/garante/doc.jsp?ID=45900; ancora, G. RASI nell'ambito del Convegno: "La sicurezza partecipata: coordinamento e cooperazione interistituzionale" svoltosi all'interno nell'ambito del Forum P.A. 2004: " <<La preoccupazione istituzionale dell'Autorità Garante per la protezione dei dati personali si è focalizzata sulla necessità che i nuovi strumenti tecnologici, finalizzati ad una fluidificazione dei rapporti tra cittadini e Pubblica amministrazione, non confliggano con il rispetto della persona e con le garanzie di riservatezza e sicurezza dei dati personali>> (…) In particolare, adeguata attenzione dovrà essere posta nella definizione delle regole tecniche e delle misure di sicurezza che dovranno essere garantite al cittadino affinché in caso, ad esempio, di smarrimento o furto, la Carta possa essere immediatamente "invalidata" a garanzia dei dati in essa contenuti.", cfr. http://www.garanteprivacy.it/garante/doc.jsp?ID=1001758.

[416] G.U. n 277 del 25-11-1999. Consultabile su www.privacy.it/dpcm19991022.html.

[417] Cfr D.M.8-11-2007, cit consultabile anche su www.interno.it.

[418] Per un'interessante panoramica dei documenti d'identificazione in diversi paesi europei ed extraeuropei, nonostante la traduzione italiana non perfetta, cfr http://www.worldlingo.com /ma/enwiki/it/National_identification_number/1. Si evidenzia, inoltre, che il 25 ottobre 2010, hanno preso il via sei progetti pilota, inseriti nel progetto generale denominato STORK, finanziato dal

Il tema è stato già affrontato dai Garanti europei nel 2003, soffermandosi, in quella occasione, su due aspetti principali: "a) il fatto che l'impiego su scala generale di identificatori originariamente settoriali necessita di adeguate garanzie (in pratica, di un fondamento di legge così come richiesto dalla direttiva 95/46). E' il caso dell'Italia e del previsto ampliamento delle possibilità di utilizzazione del codice fiscale (va ricordato, inoltre, che, ad esempio, in Portogallo esiste un divieto costituzionale di introdurre un identificatore unico nazionale); b) i rischi di un'interconnessione 'selvaggia' fra database diversi attraverso, appunto, l'identificatore unico. Anche in questo caso devono esistere idonee garanzie legislative che vietino ai soggetti pubblici di utilizzare per finalità diverse i dati raccolti e conservati, tranne nei casi previsti specificamente dalla legge"[419].

Per quanto riguarda, più in generale, i rischi legati all'interconnessione fra banche dati della pubblica amministrazione, tutte le Autorità europee si sono opposte a forme indiscriminate di interconnessione, sottolineando che le opportunità di semplificazione e razionalizzazione offerte dallo sviluppo delle tecnologie non devono tradursi in un aumento dei controlli sui cittadini[420].

Programma europeo di Sostegno alle Politiche ICT (ICT-PSP) del Programma Quadro Competitività e Innovazione (CIP). Nell'ambito del progetto STORK è stata realizzata una piattaforma europea per l'interoperabilità delle identità elettroniche (eID) ed il 25 ottobre è stato appunto annunciato che i sei progetti piloti sono disponibili al pubblico: Autenticazione trans-frontaliera per servizi elettronici, Chat più sicura, Mobilità degli studenti, Trasmissioni elettroniche trans-frontaliere, Cambio di residenza e l'integrazione col portale dei servizi della Commissione Europea. Questa piattaforma consente ai cittadini di utilizzare il proprio identificativo elettronico nazionale in diversi Stati europei. I sei progetti piloti, avviati ufficialmente, saranno gradualmente migliorati e ne sarà verificata l'integrazione con i servizi dei portali attivi della piattaforma di interoperabilità di STORK.. Cfr. http://www.digitpa.gov.it/notizie/avviati-i-sei-progetti-pilota-di-stork-l%E2%80%99interoperabilit%C3%A0-dell%E2%80%99identit%C3%A0-elettronica-tutta-eu.

[419] E-government: il punto dei Garanti europei, Newsletter Garante Privacy 9-15 giugno 2003, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=188992.

[420] Si veda per alcuni un casi italiani di interconnessione non regolamentata F. PIZZETTI, *Sicurezza, privacy, efficienza dei servizi: come conciliare i diritti per lo sviluppo di una moderna pubblica amministrazione*, Roma, 22 novembre 2007, op cit.: sd es "Fino a qualche anno fa l'Assessore alla Sanità di una Regione italiana molto importante – la Lombardia, considerata normalmente la più moderna e la più avanzata – poteva vedere sul monitor del suo computer le cartelle sanitarie di tutti gli assistiti sul territorio regionale. Se aveva voglia di sapere se il suo vicino di casa aveva avuto un certo tipo di diagnosi dal Servizio Sanitario l'Assessore poteva saperlo. Avevano fatto quel sistema per ottenere il massimo di efficienza perché in quel modo l'Assessore – che peraltro non c'entra niente perché non sono sue le competenze tecniche – aveva la possibilità di controllare la spesa sanitaria. Il risultato era di dare tutti i dati che la Regione riceveva dal Sistema Sanitario a tutti, compreso l'Assessore. Ma è evidente che i dati che il Sistema Sanitario Regionale deve trasmettere alla Regione sono molto diversificati. In alcuni casi potranno riguardare la spesa ma non la diagnosi, non nominalmente i giorni di degenza, mentre in altri casi – che comunque faccio difficoltà ad immaginare perché la Regione non fa attività terapèutica – potranno arrivare all'individuazione più specifica del singolo paziente. Ma se io non prefiguro il contingentamento dei dati e le barriere nel sistema per pigrizia, rapidità od economicità faccio si che tutti i funzionari regionali possano accedere alle informazioni dei singoli cittadini.".

Un altro strumento di rilievo dell'e-government è il passaporto elettronico che, dal 26 ottobre 2006, viene rilasciato dalle questure ed dagli uffici consolari italiani all'estero. Il documento è dotato di un microchip ed è realizzato con particolari metodi di stampa anti contraffazione ed un microprocessore che consente la registrazione dei dati e certificati, riguardanti il titolare dello stesso e dell'Autorità che lo ha rilasciato.

Dal 19 maggio 2010, cioè dall'entrata in vigore del decreto 303/13 del 23 marzo 2010[421], è prevista l'emissione del "nuovo passaporto ordinario".

Ai sensi dell'art 2 del suddetto decreto, "nel chip sono, memorizzate, in formato interoperativo, l'immagine del volto e le impronte digitali del titolare.

Nel chip sono altresì memorizzate le informazioni, già presenti sul supporto cartaceo, relative al passaporto ed al titolare, nonché i codici informatici per la protezione ed inalterabilità dei dati e le informazioni necessarie per renderne possibile la lettura agli organi di controllo.

Gli elementi biometrici contenuti nel chip potranno essere utilizzati solo al fine di verificare l'autenticità del documento e l'identità del titolare attraverso elementi comparativi direttamente disponibili quando la legge lo prevede. I dati biometrici raccolti ai fini del rilascio del passaporto non saranno conservati in banche di dati".

Particolari meccanismi di sicurezza sono finalizzati a garantire l'autenticità, la integrità e la riservatezza dei dati contenuti nel chip.

In particolare, sono previsti due tipi di controllo degli accessi alla lettura dei dati registrati nel chip: il primo, *Basic Access Control* (BAC) per evitare la lettura dei dati senza il permesso del titolare del documento, il secondo, *Extended Access Control*, (EAC) per consentire la lettura dei file contenenti le immagini delle impronte ai soli soggetti autorizzati dallo stato emettitore.

Il sistema BAC è un meccanismo di protezione dell'accesso, prescritto dall'ICAO (*International Civil Aviation Organization*), che impedisce di leggere a distanza i dati registrati sul microchip RFId del documento d'identità

[421] Consultabile su http://www.governo.it/GovernoInforma/Dossier/passaporto_ordinario/decreto_23_marzo_2010.pdf. Cfr. anche il Regolamento (CE) n. 444/2009 del Parlamento europeo e del Consiglio, del 28 maggio 2009 , che modifica il regolamento (CE) n. 2252/2004 del Consiglio relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri, GUUE L 142 del 6.6.2009, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009R0444:IT:NOT e http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:188:0127:0127:IT:PDF.

biometrico senza il permesso del titolare del documento. Per poter leggere i dati registrati sul microchip, l'apparecchio di lettura deve trasmettergli una chiave che viene calcolata in base alla data di nascita, alla data di scadenza e al numero del passaporto registrati nella MRZ (*Machine Readable Zone*) del passaporto. A questo scopo, la MRZ deve prima essere sottoposta a lettura ottica, che può essere eseguita soltanto a passaporto aperto. Appena il microchip riceve la chiave corretta si possono consultare i dati ivi contenuti, con esclusione delle impronte digitali.

Le impronte digitali sono protette, infatti, da un sistema supplementare, l'EAC [BSI1]. Il sistema EAC è un meccanismo di protezione dell'accesso, prescritto dall'UE, che impedisce agli apparecchi di lettura non autorizzati di leggere le impronte digitali registrate nei documenti d'identità biometrici. L'apparecchio di lettura può accedere alle impronte digitali soltanto se è in possesso di un certificato rilasciato dal paese emettitore del documento. Il passaporto verifica il certificato e solo in caso di validità trasmette i dati protetti.

I certificati degli apparecchi di lettura hanno una validità limitata e vanno rinnovati periodicamente. Una nazione che rilascia passaporti biometrici contenenti impronte digitali può stabilire, per mezzo dell'EAC, i Paesi o i servizi che potranno leggere le impronte digitali registrate[422].

Queste misure toccano uno degli aspetti critici del passaporto elettronico che, utilizzato prevalentemente per spostarsi da un paese all'altro, espone i dati in esso contenuti ad una diffusione anche esterna. Perciò sono necessarie, appunto, particolari cautele.

Un altro aspetto delicato del processo di emissione del passaporto è la corretta rilevazione dei dati biometrici, che deve garantire la qualità dei dati acquisiti, condizione necessaria per il successivo riconoscimento. Ciò comporta l'utilizzo di dispositivi di adeguata e certificata qualità e di procedure di acquisizione e registrazione delle impronte nel passaporto, all'atto dell'emissione dello stesso, che permettano di valutare, con l'ausilio di software di controllo, la qualità delle impronte acquisite e consentano

[422] *Tecnologie Biometriche per il controllo delle frontiere nell'Unione europea*, consultabile su http://www.cnipa.gov.it/;html/docs/BIOMETRIA%20E%20SICUREZZA%20DELLE%20FRONTIERE.pdf.

così la scelta del dito avente un' impronta con qualità maggiore per ciascuna mano, secondo una sequenza predefinita.

Riguardo alla tutela dei dati personali contenuti nei passaporti, si segnala a livello internazionale, la "Risoluzione sull'utilizzo della biometria in passaporti, carte di identità e titoli di viaggio" del 2005, in occasione della 27ma Conferenza internazionale delle Autorità di protezione dei dati e della privacy, in cui quest'ultime hanno preso atto che "governi e organismi internazionali, ed in particolare l'Organizzazione internazionale dell'aviazione civile (ICAO), stanno attualmente completando la definizione di norme e standard tecnici volti ad integrare dati biometrici (impronte digitali, riconoscimento del volto) in passaporti e titoli di viaggio ai fini della lotta al terrorismo e della velocizzazione dei controlli alle frontiere e delle procedure di imbarco".

Pertanto, le stesse Autorità chiedono che "si limiti tecnicamente l'impiego della biometria in passaporti e carte di identità alle finalità di verifica, tramite il confronto fra i dati contenuti nel documento e i dati forniti dal titolare all'atto della presentazione del documento stesso"[423].

Sempre in merito alla sicurezza dei dati raccolti in questi documenti d'identificazione, si segnalano a livello comunitario il Regolamento (CE) n. 2252/2004 del Consiglio, del 13 dicembre 2004, relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri[424], il parere del 30 settembre 2005 del Gruppo di lavoro dei garanti europei sull'attuazione del suddetto regolamento[425], le decisioni della Commissione europea C (2005) 409 del 28 febbraio 2005 e C (2006) 2909 del 28 giugno 2006, sulle caratteristiche di sicurezza rispettivamente degli elementi biometrici primari e secondari nei passaporti e nei documenti di viaggio ed, infine, il Regolamento del Consiglio dell'Unione europea n. 444/2009 del 6 maggio 2009[426], il quale modifica il precedente Regolamento del 2004.

[423] Consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1170552

[424] GUCE L 385 del 29.12.2004, pagg. 1-6, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:IT:HTML.

[425] Consultabile su http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp112_it.pdf.

[426] GUUE L 142 del 6 giugno 2009, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009R0444:IT:NOT, v, anche la relativa Rettifica, GUUE L 188/127 del 18 luglio 2009, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:188:0127:0127:IT:PDF.

Anche in questo ambito, quindi, i principi cardine richiamati sono quelli di un elevato livello di sicurezza, della qualità dei dati (i dati personali devono essere adeguati, pertinenti, non eccedenti), della legittimità dei trattamenti e dell'adeguata informazione agli interessati.

3.4. Privacy e diritto di accesso nella p.a. digitale

La disciplina generale sul procedimento amministrativo individua come principi dell'attività amministrativa, oltre all'economicità e all'efficacia, la pubblicità e la trasparenza, qualificando così il diritto di accesso come un principio generale dell'azione amministrativa.

Cosicché il problema di fondo, relativo all'applicabilità della normativa sulla tutela della riservatezza alle pubbliche amministrazioni, è basato sulla possibile contrapposizione del principio della trasparenza dell'azione amministrativa - quindi della pubblicità e conoscibilità degli atti delle pubbliche amministrazioni sancito dalla L. n. 241/90 - con il principio della tutela della riservatezza.

In quest'ambito, perciò, è stata avvertita fin dall'inizio l'esigenza di individuare un equilibrio tra queste due istanze; pertanto, non è un caso che, per la prima volta in ambito pubblico, la riservatezza sia comparsa proprio nella L. n. 241/90, dove all'art 24 è stato previsto che questa costituisce un'esigenza da salvaguardare, anche limitando il diritto di accesso, analogamente a quanto previsto anche dall'art 10 del Testo Unico degli enti locali.

La possibile conflittualità della normativa sulla privacy con quella relativa al diritto di accesso è stata affrontata anche dal Garante per la protezione dei dati personali, il quale ha precisato che la disciplina della privacy non ha abrogato il regime di pubblicità degli atti della p.a.[427]

Di contro, le amministrazioni pubbliche per lungo tempo si sono trovate nella situazione di dover valutare caso per caso quale fosse l'esigenza prevalente, svolgendo di fatto una funzione di composizione degli interessi.

[427] Garante 10 dicembre 1997, in Bollettino n. 2, pag. 50, consultabile su http://www.garanteprivacy.it/garante/ doc.jsp?ID=31039.

L'Adunanza plenaria del Consiglio di Stato, con la decisione n. 5 del 4 febbraio 1997[428], in linea con lo spirito della disciplina sulla trasparenza amministrativa, ha affermato che tale disciplina accorda prevalenza al principio di pubblicità rispetto a quello di tutela della riservatezza, consentendo l'accesso anche nei confronti di documenti contenenti dati riservati, sempre che l'istanza ostensiva sia sorretta dalla necessità di difendere i propri interessi giuridici e con il limite modale della sola visione, non essendo percorribile la modalità più penetrante e potenzialmente lesiva dell'estrazione di copia.

Con riferimento, invece, all'accesso a documenti amministrativi contenenti dati sensibili, il D.lgs. 11 maggio 1999, n. 135, integrando la L. n. 675/96 sul trattamento di questi dati da parte dei soggetti pubblici (art. 22), ha colmato il vuoto normativo determinato dall'assenza di una espressa previsione legislativa[429], chiarendo che quando la richiesta ha ad oggetto dati sensibili idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito solo se il diritto da far valere o difendere nella difesa in sede amministrativa o giudiziaria, "è di rango almeno pari a quello dell'interessato"[430].

Le norme a tutela della riservatezza, come noto, sono state successivamente rielaborate nel nuovo Testo unico sulla privacy, il quale ha previsto[431] che senza il consenso dell'interessato, il trattamento dei dati da parte della p. a. possa avvenire esclusivamente per lo svolgimento di funzioni istituzionali e che il solo trattamento dei dati non sensibili possa realizzarsi anche senza un'espressa previsione normativa. I dati sensibili e

[428] Cons. di Stato, Ad. Plen., n.5/1997, in Foro Amministrativo, 1997, p.423.

[429] Prima dell'intervento legislativo un orientamento giurisprudenziale aveva introdotto il cosiddetto "un regime a doppio binario", in virtù del quale occorreva distinguere l'ipotesi in cui la domanda di accesso riguardasse documenti contenenti dati personali non sensibili rispetto al caso in cui, invece, la domanda avesse per oggetto dati sensibili. Nella prima ipotesi trovava applicazione l'art. 24, co. 2 let. d), della legge 241/90 ed il contrasto tra diritto di accesso e tutela della riservatezza trovava composizione secondo i principi posti dalla decisione 5/97 dell'Adunanza Plenaria, nel secondo caso, invece, in assenza di una legge che specificamente consenta l'accesso, l'esigenza di tutela della riservatezza prevaleva in modo rigido ed assoluto anche sul diritto alla difesa in giudizio garantito dall'art. 24 della Costituzione. Cfr A. FERRUCCI, *Diritto di accesso e riservatezza: osservazioni sulle modifiche alla l. 241/90*, consultabile su http://www.giustamm.it/new_2005/ART_2005.htm; G. P. CIRILLO, *Diritto all'accesso e diritto alla riservatezza: un difficile equilibrio mobile*, in www.giustizia-amministrativa.it.

[430] Sui "diritti di pari rango" vedi nota 285. Cfr. Cons. Stato, sez. VI, 30 marzo 2001, n. 1882 e 9 maggio 2002, n. 2542; Cons. Stato sez. V, 31 dicembre 2003, n. 9276.

[431] Capo II, Decreto legislativo 30 giugno 2003, n. 196, cfr http://www.garanteprivacy.it/garante/doc.jsp?ID=1311248.

giudiziari sono sottoposti allo stesso regime già previsto dall'art. 22 della legge n. 675/96 dopo la riforma del '99.

Tuttavia, sotto il profilo del bilanciamento tra diritto di accesso e diritto alla privacy, il legislatore non ha abbandonato l'impostazione affermatasi sotto il vigore dei precedenti interventi normativi in materia.

L'art. 59 del Codice ha previsto espressamente, infatti, sia per i dati personali in genere che per quelli sensibili e giudiziari, che il diritto di accesso trovi la sua disciplina nella legge n. 241/90 e successive modifiche e nelle altre leggi in materia e relativi regolamenti di attuazione, mentre l'art. 60 del Codice pone una tutela differenziata e specifica per i dati relativi alla vita sessuale ed alla salute. Questi possono essere oggetto del diritto di accesso solo se l'istanza sottenda una situazione giuridica di rango almeno pari ai diritti dell'interessato, ovvero che consista in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Dall'altra parte, l'art 24 della l. 241/90 è stato modificato dalla L. n. 5/2005. La nuova formulazione, sicuramente più in linea con la disciplina del Codice in materia di protezione dei dati personali, dopo aver direttamente previsto ipotesi generali di esclusione del diritto di accesso, ha statuito che il Governo può prevedere casi di sottrazione all'accesso di documenti amministrativi, oltre ai casi già esaminati.

Questo, in particolare, può avvenire quando i documenti riguardano la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni, con specifico riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all'amministrazione dagli stessi soggetti cui si riferiscono e quando i documenti riguardino l'attività in corso di contrattazione collettiva nazionale di lavoro e gli atti interni connessi all'espletamento del relativo mandato.

"Deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici. Nel caso di documenti contenenti dati sensibili e giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall'articolo 60 del decreto legislativo 30

giugno 2003, n. 196, in caso di dati idonei a rivelare lo stato di salute e la vita sessuale"[432].

In questo quadro normativo, così indicato, si inserisce il processo di digitalizzazione della pubblica amministrazione. In particolare, il Codice dell'amministrazione digitale, come evidenziato, si è prefisso l'obiettivo di assicurare, attraverso l'applicazione che ne faranno lo Stato, le Regioni e le autonomie locali, la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale, utilizzando appunto le tecnologie dell'informazione e della comunicazione[433].

Così, nel rispetto delle disposizioni in materia di protezione dei dati personali e della vigente normativa sul procedimento amministrativo è consentito a chiunque vi abbia interesse di accedere ai documenti amministrativi, mediante l'uso delle tecnologie informatiche[434].

---

[432] Cfr. http://www.urp.it/allegati/Legge_241_modificata_2.pdf ; A. FERRUCCI, *Diritto di accesso e riservatezza: osservazioni sulle modifiche alla l. 241/90*, op cit. ; P. POZZANI, *Nuovi profili del diritto di accesso dopo la L.15/05*, consultabile su http://www.giustizia-amministrativa.it/documentazione/20050913Pozzani.htm; cfr, fra i tanti, A. CENICCOLA, *Il diritto di accesso dopo la legge n. 15/2005*, consultabile in www.lexitalia.it; A. FERRUCCI, *Diritto di accesso e riservatezza: osservazioni sulle modifiche alla l. 241/90*,op. cit. , Speciale sulla riforma della L.241/1990; F. SATTA, *La riforma della legge 241/90: dubbi e perplessità*, in www.giustamm.it, Speciale sulla riforma della L.241/1990; M. A. SANDULLI, *Accesso alle notizie e ai documenti amministrativi (sub voce)*, in Enc. Dir., IV, Aggiorn., Milano 2000, p. 19 e *Il Procedimento*, in S. CASSESE (a cura di), *Trattato di diritto amministrativo*, Tomo II, Giuffrè, Milano, 2003, p. 1165 ss.; M. CLARICH, *Trasparenza e diritti della personalità nell'attività amministrativa*, intervento al Convegno "Trasparenza e protezione dei dati personali nell'azione amministrativa", Roma, 11 febbraio 2004, in www.giustizia-amministrativa.it.; V. CERULLI IRELLI - *Osservazioni generali sulla legge di modifica della L. n. 241/*90 - I parte, in www.giustamm.it, Speciale sulla riforma della L.241/1990.

[433] Questo uno schema dei diritti del cittadino previsti (almeno sulla carta) dal Codice dell'amministrazione digitale (http://www.digitpa.gov.it/sites/default/files/CAD_lgs_235_2010.pdf):

- Diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato (articolo 2);
- diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni centrali e con i gestori di pubblici servizi statali (articolo 3);
- diritto ad esercitare, mediante l'uso delle tecnologie dell'informazione e della comunicazione, la partecipazione al procedimento amministrativo e il diritto di accesso ai documenti amministrativi (articolo 4);
- diritto ad effettuare i pagamenti spettanti alle pubbliche amministrazioni centrali con l'uso delle tecnologie dell'informazione e della comunicazione (articolo 5);
- diritto a scambiare documenti e informazioni con le pubbliche amministrazioni mediante posta elettronica certificata (articolo 6);
- diritto all'ascolto delle reali esigenze, rispetto ai servizi forniti dalle amministrazioni, ed alla misura della relativa soddisfazione (articolo 7);
- diritto alla partecipazione al processo democratico mediante l'uso delle nuove tecnologie (articolo 9);
- diritto a trovare on line tutti i moduli e i formulari validi e aggiornati ed eventualmente a concludere i relativi procedimenti in caso di loro assenza (articolo 57).

Cfr http://www.cronache-egovernment.it/?p=774;

[434] Vedi in generale il capo V, Dati delle pubbliche amministrazioni e servizi in rete, del Codice dell'amministrazione digitale, cit.

Di una certa rilevanza, poi, è il nuovo contenuto previsto per la comunicazione di avvio dei procedimenti amministrativi. Ai sensi dell'art. 8 della L. n. 241/90, infatti, questa deve indicare ai diretti destinatari le modalità per esercitare in via telematica i diritti di presa visione dei documenti e per la presentazione di memorie scritte.

D'altro canto è già la stessa riforma della L. 241/90, operata dalla l. n.15/2005, ad essere indirizzata nel senso del dominio della telematica nei procedimenti amministrativi: si veda, ad esempio, quanto previsto dall'art.3-bis della l.241/90 secondo cui, per conseguire maggiore efficienza nelle loro attività, le amministrazioni pubbliche incentivano l'uso della telematica e della comunicazione digitale. Uso che, con l'entrata in vigore del nuovo Codice dell'amministrazione digitale[435], connoterà sempre più i rapporti interni tra le diverse amministrazioni e tra queste ed i privati.

3.5. L'accessibilità in rete dei dati: il caso della pubblicazione on line delle dichiarazioni dei redditi

Nei precedenti paragrafi, si è visto come lo sviluppo dell'e-government ed, in particolare, dell'uso delle nuove tecnologie ha notevolmente facilitato l'accessibilità alle diverse informazioni, possedute dalle pubbliche amministrazioni, e la trasparenza dei procedimenti.

Il risvolto della medaglia di questi pur indubbi benefici è il pericolo che possa essere lesa anche involontariamente la riservatezza dei cittadini, che forniscono (e spesso devono fornire) quelle stesse informazioni alle amministrazioni.

Proprio al fine di evitare queste situazioni, il 15 dicembre 2010, il Garante della privacy ha approvato in via preliminare lo schema delle "Linee guida in materia di trattamento di dati personali effettuato da soggetti pubblici per finalità di pubblicazione e di diffusione sul web di atti e documenti adottati dalle pubbliche amministrazioni"[436]. Prima

[435] Cfr www.governo.it/.../Codice_amministrazione_digitale/Nuovo_CAD.ppt

[436] Il testo dello schema, sottoposto a consultazione, è visionabile su http://www.garanteprivacy.it/garante/doc.jsp?ID =1773728; Il testo definitivo è stato pubblicato il 2 marzo 2011, G. U. n. 64 del 19 marzo 2011, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1793203

dell'adozione definitiva, l'Autorità ha aperto una consultazione pubblica che si è conclusa il 31 gennaio 2011.

Le suddette Linee guida hanno scopo di definire un primo quadro unitario di misure e accorgimenti finalizzati a individuare opportune cautele che i soggetti pubblici sono tenuti ad applicare in relazione alle ipotesi in cui, secondo le disposizioni vigenti, effettuano attività di comunicazione o diffusione di dati personali sui propri siti istituzionali per finalità di trasparenza, pubblicità dell'azione amministrativa, nonché di consultazione di atti su iniziativa di singoli soggetti.

Tale intervento è dovuto anche al fatto che, soprattutto nella fase iniziale di questo processo, uno dei rischi maggiori consiste spesso nel mancato coordinamento della nuova disciplina sull'amministrazione digitale con quella precedente e con le strutture organizzative delle singole amministrazioni, non pronte al cd "salto tecnologico"[437] .

Un caso esemplificativo è stato quello riguardante la recente pubblicazione on line delle dichiarazioni dei redditi.

Prima di illustrare la questione, si deve evidenziare che la mole dei dati, di cui il fisco ha disponibilità, aveva fatto emergere la preoccupazione per la riservatezza dei dati fiscali molto prima che fosse introdotta in Italia una normativa generale sulla tutela dei dati personali[438]. Non è stata un caso, ad esempio, l'istituzione di una Commissione di vigilanza sull'anagrafe tributaria fin dalla sua nascita.

[437] Cfr F. PIZZETTI, *Sicurezza, privacy, efficienza dei servizi: come conciliare i diritti per lo sviluppo di una moderna pubblica amministrazione*, Roma, 22 novembre 2007, op cit..

[438] Da un punto di vista comparatistico si osserva che vi è una grande differenza fra i diversi Stati riguardo la riservatezza o meno dei dati dei contribuenti. Si pensi, ad esempio, alla Finlandia dove qualsiasi persona interessata alla situazione fiscale di un contribuente può chiedere tale informazione persino per sms (notizia riportata dal quotidiano La Repubblica il 2 maggio 2008). Gli Stati, inoltre, sono soliti concludere convenzioni (generalmente bilaterali) per evitare la doppia imposizione e l'evasione fiscale. Questi accordi si ispirano in particolare al modello internazionale definito dall'Organizzazione per lo sviluppo e la cooperazione in Europa (OCSE), il quale disciplina all'art. 26 lo scambio di informazioni. In particolare l'articolo consente agli Stati membri di scambiarsi informazioni, generalmente su richiesta, limitando però tale possibilità in alcune ipotesi, ad esempio quando le informazioni " non potrebbero essere ottenute in base alla propria legislazione o nel quadro della propria normale prassi amministrativa o di quelle dell'altro Stato contraente". Le informazioni ricevute, saranno comunque tenute segrete e "comunicate soltanto alle persone o autorità (ivi compresi i tribunali e gli organi amministrativi) incaricate dell'accertamento o della riscossione delle imposte previste dalla Convenzione, delle procedure o dei procedimenti concernenti tali imposte, o delle decisioni di ricorsi presentati per tali imposte. Dette persone o le predette autorità utilizzeranno tali informazioni soltanto per questi fini.. Esse potranno servirsi di queste informazioni nel corso delle udienze pubbliche di tribunale e nei giudizi". Cfr Modello di convenzione OCSE, consultabile su http://browse.oecdbookshop.org/oecd/pdfs/browseit/2310081E.PDF. Il testo delle convenzioni dell'Italia per evitare doppie imposizioni è consultabile sul sito del Ministero delle Finanze, www.finanze.it.

Inoltre, dal combinato disposto degli articoli 68 e 69 del D.P.R. n. 600/73 si poteva desumere un regime di segretezza per tutti i dati che si riferivano alla fase di accertamento tributario, mentre, per i dati forniti dal contribuente stesso, in sede di dichiarazione, era previsto che venissero depositati annualmente gli elenchi dei contribuenti - per il periodo di un anno – presso gli uffici del Comune interessato e le Amministrazioni competenti e che questi elenchi, con l'indicazione dei redditi dichiarati, fossero consultabili da chiunque ne facesse richiesta.

Quindi, la normativa fiscale, precedente l'introduzione della legge sulla tutela dei dati personali, prevedeva la garanzia della riservatezza dei dati acquisiti soprattutto nella fase di controllo[439].

Bene, la vicenda in oggetto ha origine dal fatto che, il 5 marzo 2008, il direttore generale dell'Agenzia dell'Entrate, individuando le modalità e i termini di formazione degli elenchi relativi all'anno di imposta 2005, ha disposto anche la pubblicazione di tali elenchi in un'apposita sezione del sito internet (http://www.agenziaentrate.gov.it). Così, il 30 aprile 2008 è stato pubblicato on line l'elenco delle dichiarazione dei redditi dei contribuenti, relative all'anno 2005.

Immediatamente dopo, al Garante per la protezione dei dati personali sono arrivate numerose segnalazioni di violazione del diritto alla riservatezza. Perciò, sempre il 30 aprile, l'Autorità è intervenuta bloccando l'ulteriore pubblicazione on line degli elenchi da parte dell'Agenzia delle Entrate ed aprendo, contemporaneamente, un'istruttoria sull'accertamento della legittimità di tale modalità di pubblicazione[440].

In questo provvedimento il Garante ha ribadito che la base giuridica della pubblicazione degli elenchi dei contribuenti è costituita dall'art. 69 del D.P.R.. 29 settembre 1973, n. 600, con la previsione di "una precisa scelta normativa di consultabilità da parte di chiunque di determinate fonti (…) operata per favorire una trasparenza in materia di dati raccolti dalla pubblica amministrazione attraverso le dichiarazioni fiscali"[441].

---

[439] Per un approfondimento sulla tematica del rapporto fra diritto tributario e privacy si veda, E. TRAVERSA e G. D'ANGELO, *Diritto tributario e privacy: un binomio critico*, in L BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, op cit, pag 229 e sgg.

[440] Provvedimento consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1510761.

[441] Vedi Provv. 17 gennaio 2001, doc. web n. 41031, Provv. 2 luglio 2003, doc. web. n. 1081728, nonché Provv. 18 ottobre 2007, doc. web. n. 1454901.

Inoltre, l'Autorità garante ha ricordato che non esiste incompatibilità fra il principio di trasparenza, inteso in questo caso nella determinazione di specifiche forme di pubblicità dei dati per finalità di interesse pubblico, e la protezione dei dati personali.

Ciò premesso il provvedimento ha rilevato che, mentre è compito dell'Amministrazione finanziaria la determinazione degli elenchi dei contribuenti, è invece la legge nell'art. 69 comma 6 citato a prescriverne il regime di pubblicità, individuato nel loro deposito, per la durata di un anno, ai fini della consultazione, sia presso l'ufficio dell'amministrazione finanziaria, sia presso i Comuni interessati.

Terminata l'istruttoria, il Garante, con provvedimento del 6 maggio 2008[442], ha confermato quanto stabilito precedentemente in via provvisoria. In particolare, ha rilevato che la diffusione tramite internet degli elenchi dei contribuenti disposta dall'Agenzia delle Entrate non solo è in contrasto con la normativa attualmente vigente, ma è avvenuta anche con un mezzo sproporzionato rispetto alla finalità della conoscibilità di questi dati.

L'uso di uno strumento come Internet rende indispensabili rigorose garanzie a tutela dei cittadini. Infatti, secondo quanto riscontrato:

"1) il provvedimento del Direttore dell'Agenzia poteva stabilire solo 'i termini e le modalità' per la formazione degli elenchi. La conoscibilità di questi ultimi è infatti regolata direttamente da disposizione di legge che prevede, quale unica modalità, la distribuzione di tali elenchi ai soli uffici territorialmente competenti dell'Agenzia e la loro trasmissione, anche mediante supporti magnetici ovvero sistemi telematici, ai soli comuni interessati, in entrambi i casi in relazione ai soli contribuenti dell'ambito territoriale interessato. Ciò, come sopra osservato, ai fini del loro deposito per la durata di un anno e della loro consultazione -senza che sia prevista la facoltà di estrarne copia- da parte di chiunque (art. 69, commi 4 ss., D.P.R.. n. 600/1973 cit.; v. anche art. 66 bis D.P.R.. 26 ottobre 1972, n. 633);

2) il Codice dell'amministrazione digitale, invocato dall'Agenzia a sostegno della propria scelta, incentiva l'uso delle tecnologie dell'informazione e della comunicazione nell'utilizzo dei dati delle pubbliche amministrazioni. Tuttavia, il Codice stesso fa espressamente salvi i limiti alla

[442] Pubblicato nella G.U. n. 107 dell'8 maggio 2008 e consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1512255.

conoscibilità dei dati previsti da leggi e regolamenti (come avviene nel menzionato art. 69), nonché le norme e le garanzie in tema di protezione dei dati personali (artt. 2, comma 5 e 50 D.lgs. 7 marzo 2005, n. 82);

3) la predetta messa in circolazione in Internet dei dati, oltre a essere di per sé illegittima perché carente di una base giuridica e disposta senza metterne a conoscenza il Garante, ha comportato anche una modalità di diffusione sproporzionata in rapporto alle finalità per le quali l'attuale disciplina prevede una relativa trasparenza. I dati sono stati resi consultabili non presso ciascun ambito territoriale interessato, ma liberamente su tutto il territorio nazionale e all'estero. L'innovatività di tale modalità, emergente dalle stesse deduzioni dell'Agenzia, non traspariva dalla generica informativa resa ai contribuenti nei modelli di dichiarazione per l'anno 2005. L'Agenzia non ha previsto 'filtri' nella consultazione on-line e ha reso possibile ai numerosissimi utenti del sito salvare una copia degli elenchi con funzioni di trasferimento file. La centralizzazione della consultazione a livello nazionale ha consentito ai medesimi utenti, già nel ristretto numero di ore in cui la predetta sezione del sito web è risultata consultabile, di accedere a innumerevoli dati di tutti i contribuenti, di estrarne copia, di formare archivi, modificare ed elaborare i dati stessi, di creare liste di profilazione e immettere tali informazioni in ulteriore circolazione in rete, nonché, in alcuni casi, in vendita. Con ciò ponendo anche a rischio l'esattezza dei dati e precludendo ogni possibilità di garantire che essi non siano consultabili trascorso l'anno previsto dalla menzionata norma".

Inoltre, l'Autorità ha constatato la mancata richiesta allo stesso del parere preventivo prescritto per legge[443].

Il Garante ha, altresì, specificato che va ritenuta illecita anche l'eventuale ulteriore diffusione dei dati dei contribuenti da parte di chiunque li abbia acquisiti, anche indirettamente, dal sito internet dell'Agenzia. Tale ulteriore diffusione può esporre a conseguenze di carattere civile e penale.

L'Autorità ha sottolineato, poi, che, qualora il Parlamento e il Governo ritenessero opportuno modificare la normativa alla luce del mutato scenario tecnologico, si porrà l'esigenza di individuare, sentita l'Autorità, "soluzioni

[443] art. 154, comma 4, del Codice privacy.

che consentano un giusto equilibrio tra forme proporzionate di conoscenza dei dati dei contribuenti e la tutela dei diritti degli interessati".

Il Garante ha stabilito, infine, di contestare all'Agenzia, con separato provvedimento, l'assenza di un'idonea informativa ai contribuenti riguardo alla forma adottata per la diffusione dei loro dati, anche al fine di determinare la relativa sanzione amministrativa.

L'epilogo della vicenda è segnato dall'intervento, appunto, del legislatore, il quale da un lato ha modificato l'art 69 D.P.R.. n. 600/73 in chiave maggiormente garantista e, dall'altra, è intervenuto sul sistema sanzionatorio a tutela della riservatezza anche dei dati reddituali dichiarati.

In particolare, il nuovo art. 69 ha condizionato il diritto alla consultazione degli elenchi ai presupposti generali, previsti dalle norme in materia di accesso contenute nella L. n. 241/90, limitandolo, quindi, in maniera rilevante rispetto alla precedente disciplina[444].

Al di là del rilevato interesse della vicenda, per quel che riguarda agli aspetti applicativi e di coordinamento delle nuove tecnologie nelle pubbliche amministrazione e del necessario bilanciamento con la tutela dei dati personali del cittadino, si sottolinea il caso anche come evidente esempio dell'importanza del ruolo che ha e avrà il Garante nel discriminare ciò che è lecito da ciò che non lo è, nel campo della tutela della privacy. Ruolo che si presenta particolarmente rilevante soprattutto laddove non vi sia una disciplina normativa specifica, come spesso può accadere nel settore delle nuove tecnologie.

L'incisività dell'intervento si manifesta, come visto, anche nei rapporti con gli organi istituzionali, "suggerendo" scelte di politica legislativa,

[444] Art 69 D.P.R.. 600/73 "(…) 5. Con apposito decreto del Ministro delle finanze sono annualmente stabiliti i termini e le modalità per la formazione degli elenchi di cui al comma 4.

6. Gli elenchi sono depositati per la durata di un anno sia presso lo stesso ufficio delle imposte, sia presso i Comuni interessati. Nel predetto periodo è ammessa la visione e l'estrazione di copia degli elenchi nei modi e con i limiti stabiliti dalla disciplina in materia di accesso ai documenti amministrativi di cui agli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e successive modificazioni, dalla relativa normativa di attuazione, nonché da specifiche disposizioni di legge. Per l'accesso non sono dovuti i tributi speciali di cui al decreto del Presidente della Repubblica 26 ottobre 1972, n. 648 . 6-bis. Fuori dei casi previsti dal comma 6, la comunicazione o diffusione, totale o parziale, con qualsiasi mezzo, degli elenchi o di dati personali ivi contenuti, ove il fatto non costituisca reato, è punita con la sanzione amministrativa del pagamento di una somma da cinquemila euro a trentamila euro. La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore. 7. Ai comuni che dispongono di apparecchiature informatiche, i dati potranno essere trasmessi su supporto magnetico ovvero mediante sistemi telematici.". Testo consultabile su http://www.miolegale.it/normativa/253-Accertamento-imposte-redditi-dpr-600-1973/8.html.

indirizzate verso soluzioni ritenute maggiormente compatibili con la normativa a tutela dei dati personali.

Sempre in merito ai dati fiscali, si segnala, infine il provvedimento del Garante del 30 settembre 2008, relativo alle misure di sicurezza prescritte per gli accessi all'Anagrafe Tributaria[445]. Quest'ultima costituisce, infatti, un complesso sistema informativo al quale ha accesso - attraverso diversi strumenti telematici (applicativi Siatel, Puntofisco, Entratel, servizi web etc.) - un numero enorme di utenti, tra i quali, Comuni, Regioni, Province, Università, Asl, Tribunali, Camere di commercio, enti previdenziali, gestori telefonici, forze di polizia, con migliaia di punti di accesso.

Per questo motivo il Garante ha ritenuto opportuno verificare la sussistenza di garanzie per la tutela del trattamento di tali dati, riscontrando, invece, diverse carenze, quali: mancata conoscenza del numero complessivo degli utenti che accedono al sistema informativo e della loro effettiva identità; scarsa capacità di monitoraggio su eventuali accessi anomali o utilizzi impropri di password e credenziali; inadeguate misure tecnologiche a protezione dei dati contenuti nel data base.

Per porre rimedio a tali assenze l'Autorità ha imposto all'Agenzia delle Entrate l'adozione di numerose misure entro un termine che va dai tre mesi ad un anno in relazione alla complessità degli adempimenti.

In particolare, le misure hanno riguardato la regolamentazione degli accessi (es. ricognizione periodica degli accessi, blocco degli accessi non autorizzati, censimento aggiornato di tutti i flussi di trasferimento dei dati da e verso l'Agenzia, compartimentazione - cronologica, geografica, per tipologia - dei dati visualizzabili, adozione di sistemi di allarme per eventuali comportamenti anomali) e i sistemi di autenticazione (es. censimento delle postazioni dei terminali dai quali si ha accesso ai dati, adozione di sistemi di "autenticazione rafforzata" – ovvero password a scadenza immediata, tessere *smart card* dotate di pin - implementazione di un sistema di certificazione digitale per gestire l'identità elettronica dei sistemi informatici e degli utenti della banca dati[446]).

Infine, le misure prescritte nel provvedimento hanno riguardato le abilitazioni e autorizzazioni agli utenti: fra gli altri, il tracciamento degli

[445] http://www.garanteprivacy.it/garante/doc.jsp?ID=1549526.

[446] Tutti esempi questi di utilizzo della tecnologia per tutelare la privacy, cd *privacy enhancing tecnologies*.

utenti che accedono via web, la gestione dei flussi di dati su canali di connessione sicuri.

Anche quest'ultimo è un esempio indicativo della rilevanza dell'attività del Garante nello stabilire la disciplina dell'attività di trattamento dei dati, affinché questa sia svolta correttamente, soprattutto in quei settori specifici, non disciplinati né con normativa di livello primario né con normativa di livello secondario.

4. Privacy e Comunicazioni elettroniche

Ai sensi dell'art 4 comma 2 del Codice in materia di protezione dei dati personali, per comunicazione elettronica si intende "ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico"[447]. Le comunicazioni elettroniche sono disciplinate dal Titolo X del D.lgs. n. 196/03, nonché dal d.lgs. n. 259/2003, Codice delle comunicazioni elettroniche.

Secondo la definizione del Codice delle comunicazioni elettroniche, per reti di comunicazione elettronica si intendono "i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse, a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato"[448].

L'applicazione delle tecnologie alla comunicazione ha fatto sì che oggi una mole immensa di informazioni passi attraverso i canali di comunicazione elettronica, tanto da caratterizzare sempre di più la stessa

[447] Il Codice delle comunicazioni elettroniche definisce all'art. 1, *aa)* la rete pubblica di comunicazione come "una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico".

[448] D.lgs. n. 259/2003, *Gazzetta Ufficiale* n. 214 del 15 settembre 2003 - Supplemento Ordinario n. 150, consultabile su http://www.parlamento.it/parlam/leggi/deleghe/03259dl.htm. Il codice ha dato attuazione alla direttiva 2002/21/CE.

organizzazione sociale, come società basata sull'accumulazione e la circolazione (soprattutto elettronica) dell'informazione. Questo ha comportato la nascita di una vera e propria nuova risorsa, l'informazione stessa, alla quale si collega lo stabilirsi di nuove forme e di nuove situazioni di potere, così da poter parlare di società dell'informazione, di *electronic partecipation*, di cittadinanza elettronica, di *networked people* [449]ecc.

Le tecnologie elettroniche, con la possibilità di organizzare, unificare e far permanere informazioni disperse o destinate a scomparire, hanno introdotto anche un nuovo modo di costruzione della sfera privata[450], senza contare che il continuo sviluppo della scienza ha fatto in modo che le nuove tecnologie si presentino con un pervasività sempre maggiore, spesso associata alla loro non visibilità: forniamo informazioni spesso inconsapevolmente.

Per questo si è parlato anche di società della sorveglianza, in cui quest'ultima rappresenterebbe ormai la forma propria della società dell'informazione: "una sorveglianza pervasiva, che si esercita su corpi profondamente mutati dall'immersione nel fluire delle comunicazioni elettroniche, e che si dirama e si diffonde ovunque"[451], riproponendo il modello del *Panopticon* di Jeremy Bentham[452].

In questo contesto, si comprende bene, allora, come il tema della privacy sia parte integrante della più generale dimensione della garanzia delle libertà fondamentali, dei diritti civili e della stessa organizzazione democratica della società.

Le reti di comunicazione elettronica mettono, poi, in evidenza un altro degli aspetti che caratterizza la "società globale dell'informazione": la transnazionalità. Intesa questa non solo in riferimento alle tematiche, ma anche, ad esempio, agli illeciti, i quali possono essere compiuti sul territorio da soggetti situati al di fuori dei confini nazionali e, quindi, fuori dal controllo dell'autorità statale.

[449] S. RODOTà, *Tecnologia e diritti*, op cit. pag. 33.

[450] S. NIGER, *Le nuove dimensioni della privacy*, op. cit. pag.67.

[451] D. LYON, *la società sorvegliata. Tecnologie di controllo della vita quotidiana*, con introduzione di S. RODOTà, Feltrinelli 2002; S. NIGER, *Le nuove dimensioni della privacy*, op. cit. pag. 169 e ss; S. RODOTà, *Libertà personale. Vecchi e nuovi nemici*, in M. BOVERO. (a cura di), Quale libertà. Dizionario minimo contro i falsi liberali, op. cit.

[452] J. BENTHAM, *Panopticon* ,1797, trad. it. di V. FORTUNATI, Padova, 1983.

Pertanto, una risposta alla necessità di bilanciare tecnologie e tutela dei dati personali che aspiri ad essere davvero efficace, non può prescindere da questo aspetto, ma deve presentarsi, anche e soprattutto, come frutto di un'intelligente cooperazione internazionale.

In questo settore, si assiste, alla presenza di due linee di sviluppo, l'una definita "*user-centered*"[453], per cui i sistemi e i servizi di telecomunicazione mettono al centro l'utente in modo da fornirgli con semplicità tutti i servizi di cui questi può avere bisogno ovunque si trovi e consentendo una comunicazione prima inimmaginabile.

L'altra, invece, è denominata "*device-less*"[454] ed indica come la tecnologia si presenta sempre più pervasiva e nascosta. Ne è un esempio la cosiddetta "*smart dust*" o "polvere intelligente", in cui si integrano tutte le funzionalità che possono interessare i servizi di comunicazione: dalla memorizzazione alla sensoristica, dai sistemi di controllo a quelli di display e anche ai sistemi di locomozione.

Fra le comunicazioni elettroniche rientrano ovviamente gli strumenti di comunicazione tradizionali, quali il telefono ed il fax, tuttavia, in questa sede ci si soffermerà sulle nuove tecnologie come internet - il sistema di comunicazione che si è più velocemente evoluto ed imposto in questi ultimi anni – e le tecnologie *ubiquitous computing* - in particolare le tecnologie Rfid e la geolocalizzazione - soprattutto in riferimento ad alcune delle problematiche connesse al loro rapporto con il diritto alla privacy.

4.1. Internet

Oggi internet si manifesta sempre più nettamente come un potente strumento di trasformazione della società, tanto che rischiare di rimanere

[453] La *User-Centered Design* (UCD) è una metodologia composta da una serie di differenti tecniche e attività interattive che consentono di sviluppare prodotti che, nell'interazione uomo-macchina, tengano conto, fin dalle prime fasi di ideazione, dei bisogni, delle aspettative e delle possibili limitazioni dell'utente finale. La filosofia che guida questa metodologia è l'attenzione posta non solo alle potenzialità e alle caratteristiche del prodotto tecnologico, ma anche e soprattutto alle persone che utilizzeranno tale prodotto, in modo da favorirne il miglior utilizzo possibile.
La UCD nasce e si sviluppa in ambito informatico come tecnica destinata a migliorare la creazione di portali e applicazioni web-based, rendendoli effettivamente adeguati alle conoscenze e al contesto d'uso degli utenti.Uno standard internazionale che definisce le basi di molte tecniche di UCD è la norma ISO 13407 - Human-centred design process. Vedi http://www.cineca.it/pagine/ucd_uxlab.htm.

[454] F. VATALARO, *Privacy e sicurezza in ambito wireless*, Convegno"Innovazioni tecnologiche e privacy. Sviluppo economico e progresso civile ", Roma 17-18 giugno 2004, pag 166 consultabile su http://www.garanteprivacy.it/ garante/document?ID=1595454.

abbagliati da quella che è stata chiamata *Internet Trinity*: una trinità fatta dalla tecnologia del mezzo, dalla distribuzione geografica dei suoi utenti, dalla natura dei suoi contenuti[455]. Internet ha introdotto, infatti, un modello di organizzazione a rete, in cui è davvero possibile instaurare una rete di rapporti che consentono a ciascuno di entrare in rapporto con gli altri e di essere al tempo stesso produttore e consumatore di informazioni.

Inizialmente, infatti, le informazioni in rete potevano essere definite come un vero e proprio "prodotto" frutto del lavoro di società specializzate, l'utente, quindi, in un certo senso subiva l'informazione. La successiva diffusione di soluzioni *software* e *hardware* semplici ed a basso costo, unita all'espansione delle conoscenze informatiche ha fatto sì che si facesse strada la produzione di informazioni anche dal "basso".

Si è passati, dunque, da contenuti generati da soggetti specializzati a contenuti generati dagli utenti stessi *user generated content* (UGC)[456].

Internet ha permesso così una vera e propria "rivoluzione copernicana" nei metodi di elaborazione, selezione, ricerca e spostamento dei dati, cosicché le regole di circolazione delle informazioni, anche e sempre più incisivamente in rete, oggi determinano vere e proprie forme di redistribuzione del potere all'interno della società, tanto da poter parlare del cd. "potere informatico" [457](vedi, ad esempio, il caso di *WikiLinks*).

Pur trattandosi sicuramente di una rivoluzione positiva per la libertà di espressione deve anche essere preso in considerazione che attraverso la rete viene messa in circolazione, da utenti più o meno consapevoli, un numero impressionante di informazioni, spesso riguardanti dati personali anche di altre persone, con il forte rischio di violazione della privacy individuale nonché il rischio dell'utilizzo non corretto di tale informazioni, a fini commerciali o per realizzare veri e propri reati.

Internet è uno spazio sociale, politico ed economico, ma soprattutto è uno spazio globale[458], da qui la necessità di salvaguardare anche in rete i

[455] S.RODOTà, *Relazione introduttiva al Convegno "Internet e privacy - quali regole?"*, Roma 8-9 maggio 1998, consultabile su http://www.interlex.it/675/rodotint.htm e http://www.privacy.it/garanterelrod.html per gli altri atti del Convengo si veda http://www.privacy.it/garante1998convegno.html.

[456] S. MELE, *Privacy e user generated content (UGC)*, in L BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, op cit, pag 51 e ss.

[457] S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, op. cit., pagg. 62 e ss.; S.RODOTà, *Tecnologia e diritti*, op. cit., pag 99.

[458] S.RODOTà, *Relazione introduttiva al Convegno "Internet e privacy - quali regole?"*, Roma 8-9 maggio 1998, op. cit.

diritti e le libertà fondamentali. Questo a partire per esempio dalle condizioni della connettività:

1) in teoria l'accesso è illimitato, in concreto la richiesta di acceso a costi particolari può limitarlo molto. Un esempio in tema di comunicazione televisiva: qualche anno fa in Inghilterra alcune manifestazioni sportive come la finale di Coppa di Inghilterra, il torneo di Wimbledon o il Derby di Exon sono state dichiarate una sorta di "patrimonio culturale del popolo inglese" per evitare che fossero trasmesse in forma criptata e rimanessero, invece, liberamente accessibili[459].

2) Alfabetizzazione informatica, anche in senso di capacità di uso consapevole di tali mezzi. L'educazione alla tecnologia, in questo caso l'educazione a internet, non solo rappresenta in assenza di regolamentazione la forma più efficace di autodifesa, ma anche lo strumento per consentire la diffusione di uno strumento che è ancora visto con molta diffidenza.

Per quanto riguarda, poi , la tutela della privacy in rete, si deve tenere presente che:

In rete, senza accorgimenti, non esiste privacy[460]. L'origine e la destinazione di ogni comunicazione così come il contenuto, sono identificabili presso ogni nodo di rete intermedio, con semplici tecniche di analisi del traffico.

In rete, senza accorgimenti, nessuno è completamente libero di esprimersi[461]. La pubblicazione sul web è facilmente censurabile attaccando, per via informatica o legale, un singolo server: si veda l'esempio di *Google*, *Yahoo*, *Microsfot* che hanno accettato richieste censorie da parte di stati autoritari, pena l'esclusione dai mercati come quello cinese, economicamente importantissimi. Nasce in questo modo una sorta di "censura di mercato"[462].

[459] S.RODOTà, *Relazione introduttiva al Convegno "Internet e privacy - quali regole?"*, Roma 8-9 maggio 1998, op. cit.

[460] Così G. BIANCHINI, *La sfera della privacy nell'era digitale: minacce e mezzi di difesa*, consultabile su www.giannibi.net/nottebianca.pdf.

[461] vedi nota precedente.

[462] S. RODOTà, *Internet tra sicurezza e normalizzazione*, La Repubblica 15-1-2009, consultabile su http://www.astrid-online.it/Forme-e-st/Rassegna-s/LA-REPUBBLICA_S_Rodot--15_01_09.pdf.

Queste grandi imprese come *Google* finiscono per impersonificare il "decisore globale finale" in materie che riguardano libertà e diritti, esercitando un potere non soggetto ad alcun controllo.

La questione è così rilevante che, per esempio, un gruppo di parlamentari democratici e repubblicani ha presentato al Congresso americano una proposta di legge, il *Global Online Freedom Act*[463], per obbligare tutte le società operanti su Internet a comunicare ad un nuovo ufficio del Dipartimento di Stato tutti i casi in cui hanno "filtrato" materiali su richiesta di Stati esteri, impedendo così che le principali aziende tecnologiche statunitensi possano fornire dati personali ed informazioni ai governi stranieri in relazione all' utilizzo della rete da parte dei cittadini dei rispettivi paesi.

In rete, senza accorgimenti, nessuno è anonimo[464]. Quindi, tutela della riservatezza anche come strumento di comunicazione.

Molti vedono la soluzione di tali problematiche in una strategia integrata di strumenti e soggetti (internazionali e nazionali) nel quadro di forti principi di riferimento: "l'unica strada è individuare principi forti nei quali una società possa riconoscersi perché corrispondono ai valori della democrazia, della libertà e dignità della persona", un vero e proprio *Internet Bill of Rights*[465], una "Costituzione per Internet", non una costituzione intesa in senso classico, "ma un insieme di regole, codici deontologici, intese internazionali capaci di mantenere alla Rete il suo carattere di infinito spazio di libertà"[466] .

In questa direzione si colloca anche la Risoluzione presa in occasione della 30° Conferenza Internazionale delle Autorità di protezione dei dati "sull'urgenza di tutelare la privacy in un mondo senza frontiere e di addivenire ad una proposta congiunta finalizzata alla definizione di standard internazionali in materia di privacy e protezione dei dati personali" [467].

---

[463] Cfr. http://www.govtrack.us/congress/bill.xpd?bill=h111-2271.

[464] Vedi nota 460.

[465] S. RODOTà, *Internet Bill of rights: nuovi diritti che vanno condivisi e riconosciuti*, consultabile su http://saperi.forumpa.it/story/33743/internet-bill-rights-nuovi-diritti-che-vanno-condivisi-e-riconosciuti; ancora S. RODOTà, *Una Carta dei diritti del web*, consultabile su http://www.repubblica.it/2007/11/sezioni/scienza_e_tecnologia/rodota-web/rodota-web/rodota-web.html.

[466] S. RODOTà, *Internet Bill of rights: nuovi diritti che vanno condivisi e riconosciuti*, op cit, pag. 138.

[467] Consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1566053.

Tuttavia, è stato anche evidenziato che "in nessun caso, però, devono essere regole che sfruttano l'occasione tecnologica per imporre un punto di vista ideologico o religioso. Vi è un limite nell'uso stesso del diritto, che non deve pretendere di impadronirsi della vita privata delle persone, di espropriarle della loro libertà di scelta"[468].

Si parla in tale contesto della cd. libertà informatica, intesa non solo in termini di difesa dal potere informatico, sia pubblico che privato, ma altresì "come pretesa di libertà in senso attivo , non libertà da ma libertà di, che è quella di valersi degli strumenti informatici per fornire e ottenere informazioni di ogni genere. E' il diritto di partecipazione alla società virtuale, che è stata generata dall'avvento degli elaboratori elettronici nella società tecnologica"[469].

Appare evidente, allora, come questa nuova forma "tecnologizzata" della libertà di comunicazione debba essere rapportata e confrontata con le tradizionali libertà costituzionali, in particolare con la libertà di comunicazione, appunto, e con quella di manifestazione del pensiero.

Per quanto riguarda l'espressa positivizzazione della libertà informatica, si osserva che molte costituzioni latino americane, ad esempio, contengono diverse norme che fanno esplicito riferimento a situazioni soggettive derivanti dalla tecnologia informatica[470].

Esemplare in tal senso è l'art 30 della Costituzione della Repubblica del Paraguay (1992) che recita: "La legge assicura, con uguaglianza di opportunità, il libero accesso all'utilizzo dello spettro elettromagnetico, così come degli strumenti elettronici di accumulazione ed elaborazione dell'informazione pubblica, senza altri limiti che quelli imposti dai regolamenti internazionali e dalle norme tecniche. Le autorità devono provvedere affinché questi elementi non vengano utilizzati per ferire

[468] S. Rodotà, *Intervista su privacy e libertà*, op. cit. pag 138.

[469] Così V. FROSINI, *L'orizzonte giuridico dell'Internet*, in Il diritto dell'informazione e dell'informatica, n. 2, 2002, pag. 275.

[470] Per una panoramica di queste si veda T. E. FROSINI, *Tecnologie e libertà costituzionali*, op cit. pag. 177 e ss.; dello stesso autore, *Libertà informatica come libertà costituzionale*, in Materiale selezionato dal corso di Informatica e diritto P.O.R. Campania, consultabile su http://www.unisob.na.it/e-unisob/eteca/innovazione/innovazione_4 /innovazione_4_12.pdf . Per la dottrina sulla libertà informatica nella cultura giuridica latinoamericana si rinvia a E. SANCHEZ JIMENEZ, *los derechos humanos de la tercera generatiòn: la libertad informatica*, (Comunicazione presentata al III Congresso Iberoamericano di Informatica e diritto) in Informatica y Derecho, n 3, 1992, 85 e ss; E. ROSO ACUNA, *Habeas Data costituzionale: nuova garanzia giurisdizionale del diritto pubblico latinoamericano*, in Dir. Pubb. Comparato ed europeo, n 4 2002, 1923.

l'intimità personale o familiare e gli altri diritti stabiliti in questa Costituzione"[471].

Per quanto riguarda, invece, le libertà costituzionali scritte ed affermate in periodi storici precedenti l'avvento della tecnologia informatica, si evidenzia la vicenda giurisprudenziale americana, confluita nella sentenza del 1997 della Corte Suprema relativa all'incostituzionalità della legge che vietava comunicazioni indecenti sulla rete Internet[472], in cui si rinvengono una serie di importanti osservazioni riguardo a Internet in generale e in rapporto alle libertà costituzionali.

In particolare, si riporta l'affermazione finale della sentenza, con cui è stata appunto confermata la decisione di incostituzionalità della legge, in quanto in contrasto con il Primo emendamento: "I fatti accertati dimostrano che l'espansione di Internet è stata, e continua ad essere, fenomenale. E' tradizione della nostra giurisprudenza costituzionale presumere, in mancanza di prove contrarie, che la regolamentazione pubblica del contenuto delle manifestazioni del pensiero è più probabile che interferisca con il libero scambio delle idee piuttosto che incoraggiarlo. L'interesse a stimolare la libertà di espressione in una società democratica è superiore a qualunque preteso, non dimostrato, beneficio della censura".

La sentenza, quindi, ha esaminato il fenomeno Internet come problema costituzionale evidenziandone i limiti, ma soprattutto le potenzialità ai fini di un accrescimento delle libertà ed ha estrapolato dal vecchio Primo

[471] "Artículo 30 - DE LAS SEÑALES DE COMUNICACIÓN ELECTROMAGNÉTICA

La emisión y la propagación de las señales de comunicación electromagnética son del dominio público del Estado, el cual, en ejercicio de la soberanía nacional, promoverá el pleno empleo de las mismas según los derechos propios de la República y conforme con los convenios internacionales ratificados sobre la materia.

La ley asegurará, en igualdad de oportunidades, el libre acceso al aprovechamiento del espectro electromagnético, así como al de los instrumentos electrónicos de acumulación y procesamiento de información pública, sin más límites que los impuestos por las regulaciones internacionales y las normas técnicas. Las autoridades asegurarán que estos elementos no sean utilizados para vulnerar la intimidad personal o familiar y los demás derechos establecidos en esta Constitución." Consultabile su http://www.federalismi.it/document/19112009151416.pdf e fra gli altri nel vol. *Le Costituzioni dell'America Latina*. Vol.I: *I Paesi dell'area del Mercosur*, cit., 372 ss. Vedi altresì l'art. 33 per la tutela del diritto alla riservatezza e l'art.135 sugli aspetti fondamentali del diritto-garanzia costituzionale di *habeas data*. Sul punto, vedi E. ROZO ACUNA, *Habeas Data costituzionale: nuova garanzia giurisdizionale del diritto pubblico latinoamericano*, op. cit., 1932-1933.

[472] La sentenza del 26 giugno 1997 è rinvenibile sul sito www.aclu.org ed è tradotta in italiano su Foro it., Parte IV-2, 1998, 23 e ss. Fra la dottrina italiana che al tempo se ne è occupata, v. G. ZICCARDI, *La libertà di espressione inInternet al vaglio della Corte Suprema degli Stati Uniti*, in Quaderni costituzionali, n.1, 1998, 123 ss.

Emendamento, del 1791, le forme di tutela e garanzia per la libera espressione del pensiero su Internet.

I giudici, perciò, nell'utilizzare il Primo Emendamento, come parametro per l'incostituzionalità della legge repressiva della libertà in Internet, lo hanno reinterpretato alla luce del ventesimo secolo, dando ad esso un significato che non è e non può essere quello originario e che tutela non solo il tradizionale diritto di libertà del pensiero, ma anche la libertà di parola elettronica, la libertà di stampa elettronica, la libertà di riunione elettronica.

In tal modo si afferma il diritto di libertà informatica, quale "nuovo" diritto di libertà costituzionale, ricavabile dai tradizionali diritti e principi costituzionali, che vanno letti e interpretati nel contesto della società tecnologica.

Così, spetta ai giudici, particolarmente a quelli costituzionali, il compito di saper reinterpretare la vecchia tradizione costituzionale alla luce del progresso tecnologico. A loro pertanto, "tocca il compito di saper essere 'giurista nella società tecnologica', coinvolto all'interno di essa"[473].

Per quanto riguarda l'Italia, si segnala a questo proposito che lo scorso 6 dicembre Stefano Rodotà ha presentato al Senato un disegno di legge[474], assegnato il 1 febbraio 2011 alla 1ª Commissione permanente (Affari Costituzionali) in sede referente, per l'introduzione nel testo costituzionale di un nuovo art. 21bis volto al riconoscimento del diritto di accesso ad Internet[475].

4.1.1. Quadro giuridico di riferimento

A livello internazionale va indicata, innanzitutto, la Dichiarazione ministeriale sulla protezione della privacy sulle Reti globali[476], adottata in ambito OCSE, in occasione della Conferenza ministeriale svoltasi ad

[473] Così T. E. FROSINI, *Tecnologie e libertà costituzionali*, op cit. pag. 185.

[474] DDL n 2485 http://www.senato.it/leg/16/BGT/Schede/Ddliter/36202.htm.

[475] Così S. RODOTà "Una cittadinanza amputata della dimensione digitale non è più una cittadinanza, perché esclude la persona dalla dimensione globale", in un articolo dello stesso autore, *Internet è un diritto, va scritto in Costituzione*, consultabile su http://mag.wired.it/rivista/storie/stefano-rodota-internet-e-un-diritto-che-va-scritto-nellacostituzione .html

[476] Dichiarazione ministeriale sulla protezione della privacy sulle Reti globali, DSTI/ICCP/REG(98)10/FINAL, consultabile in inglese su http://www.oecd.org/dataoecd/39/13/1840065.pdf.

Ottawa il 7-9 ottobre 1998, la quale già allora sollecitava l'esame delle questioni, specificamente concernenti la tutela della riservatezza sulle reti globali, sorte nel contesto dell'attuazione delle Linee-guida del 1980.

Le successive Linee guida sulla sicurezza dei sistemi e delle reti d'informazione, approvate sottoforma di Raccomandazione del Consiglio dell'OCSE il 25 luglio 2002, hanno messo in evidenza, poi, la necessità di una maggiore vigilanza e analisi in relazione alle sempre più urgenti questioni di sicurezza dei sistemi e delle reti d'informazione, sviluppando una vera e propria "cultura della sicurezza"[477].

In ambito europeo, come descritto nei precedenti paragrafi, con riguardo più specifico alla tutela della riservatezza nell'ambito delle comunicazioni elettroniche, la Direttiva n. 95/46 è stata integrata dalla Direttiva n. 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (cd. "direttiva e-privacy"), in seguito modificata dalla Direttiva n. 24 del 2006 e recentemente dalla Direttiva n. 136 del 2009.

La Direttiva n. 58/2002, quindi, non ha sostituito la Direttiva generale sulla protezione dei dati n. 95/46/CE, la quale, come visto, si applica a qualsiasi trattamento dei dati personali che rientri nel relativo ambito di applicazione, indipendentemente dalla tecnologia utilizzata e, pertanto, opera per tutte le tematiche non coperte dalla Direttiva del 2002 e per tutti i trattamenti con strumenti elettronici che esulano dall'applicazione di quest'ultima direttiva[478].

I principi generali stabiliti dalla Direttiva n. 95/46/CE, come quelli di finalità, di necessità, del trattamento leale e delle informazioni da fornire alla persona interessata dal trattamento, valgono, pertanto, anche per le comunicazioni elettroniche, internet incluso.

La Direttiva n. 2002/58/CE[479] ha posto poi obblighi particolari in materia di sicurezza delle comunicazioni elettroniche, come ad esempio

[477] Linee guida sulla sicurezza dei sistemi e delle reti d'informazione. Verso una cultura della sicurezza, consultabile su http://www.oecd.org/dataoecd/16/23/15582268.pdf.

[478] C. FILIPPI, *Le nuove regole per i servizi di comunicazione elettronica:l'attuazione della direttiva 2002/58. La tutela della riservatezza su internet e reti telematiche*, in G. SANTANIELLO (a cura di) La protezione dei dati personali, op. cit., pag 617; A. MANEGGIA, *La tutela della privacy nell'era delle comunicazioni elettroniche: cosa ha cambiato Internet?*, in In.Law, 2006, pp. 303-323, consultabile su www.morlacchilibri.com/inlaw/ downloads/ in.law_08_3.pdf.

[479] Cfr http://europa.eu/legislation_summaries/information_society/l24120_it.htm.

l'obbligo dei fornitori di adottare misure appropriate per salvaguardare la sicurezza dei servizi da essi offerti (art. 4) e ha previsto una serie di misure a tutela della riservatezza (art. 5), quale l'obbligo degli Stati di garantire che l'uso di reti di comunicazione elettronica, per archiviare informazioni o per avere accesso ad informazioni archiviate nell'apparecchio terminale di un utente, sia consentito unicamente a condizione che quest'ultimo ne sia stato informato in modo chiaro e completo e che gli sia offerta la possibilità di rifiutare tale trattamento, fatta salva la memorizzazione automatica, intermedia e temporanea, necessaria alla trasmissione nelle reti di comunicazione elettroniche.

Inoltre, tra le questioni giuridiche legate alle illimitate capacità di trasmissione e comunicazione consentite da Internet rientra quella di garantire la tutela della privacy e un determinato standard di protezione dei dati personali garantito dallo Stato, in una situazione in cui operatori e soggetti esteri entrino in possesso di dati e informazioni personali di individui soggetti alla giurisdizione statale[480].

Questo, infatti, rischia di vanificare la tutela fornita dalle normative se le garanzie da essi accordate non possono trovare applicazione al di fuori dei confini nazionali.

Al riguardo gli Stati hanno adottato soluzioni diverse, comportanti in alcuni casi l'applicazione extraterritoriale della normativa statale pertinente. Ad esempio, in America la legge sulla tutela dei bambini on line del 1998 (*Children's Online Privacy Protection Act*[481]) si applica anche ai siti web stranieri che raccolgono informazioni personali dai bambini sul territorio statunitense.

[480] Le questioni relative alla legge applicabile e alla giurisdizione in relazione ad atti compiuti su o tramite internet sono oggetto di approfondite analisi di diritto internazionale, sia privato che pubblico, riguardanti più in generale l'estensione della giurisdizione statale su Internet. Tuttavia, oltrepassando l'ambito della presente indagine, per esse si rinvia fra i tanti a M. WINKLER, *La giurisdizione nel ciberspazio*, in Ciberspazio e Diritto, Volume II, Numero II, pp. 197-240. Articolo tratto dal sito http://www.ciberspazioediritto.org; T. BALLARINO, *Internet nel mondo della legge*,Cedam, Padova 1998: dello stesso autore, *Diritto internazionale privato*, Cedam, Padova 1999; F. BRUGALETTA – F. M. LANDOLFI (a cura di), *Il Diritto nel Cyberspazio*, Simone, 1999; P. CERINA, *Il problema della legge applicabile e della giurisdizione*, in E. TOSI (a cura di), I problemi giuridici di Internet, Giuffrè Milano, 1999, pag. 351 ss; E. LANDOLFI, *La giurisdizione ed Internet*, Diritto e diritti n.3/99.

[481] Consultabile su http://www.ftc.gov/ogc/coppa1.htm; cfr anche http://www.coppa.org/comply.htm e http://www.ftc.gov/privacy/privacyinitiatives/childrens.html; in merito alla tutela della privacy del minore, in particolare riguardo al diritto di cronaca, si rinvia a F. RAIA, *Privacy e diritto di cronaca con riguardo a particolari categorie di soggetti: le persone pubbliche e i minori*, consultabile su http://www.associazionedeicostituzionalisti.it/dottrina/libertadiritti/raia.html.

In base alla predetta normativa, il gestore di un sito web diretto verso bambini di meno di 13 anni (o rivolto ad un pubblico più vasto, ma nell'ambito del quale il gestore sia a conoscenza della raccolta di informazioni da bambini) è obbligato ad ottemperare alle disposizioni previste nella legge del 1998. Tale disciplina, quindi, non si applica specificatamente solo alle imprese statunitensi, ma alle imprese "situate su internet" e, quindi, ai fini della giurisdizione, non rileva l'ubicazione fisica del sito web, nel caso in cui lo stesso operi negli Stati Uniti[482].

In ambito comunitario la legislazione di attuazione della Direttiva n. 95/46 emanata da uno Stato membro si applica, in base all'art. 4, lett. a), al trattamento di dai personali "effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile"; mentre ai sensi della lett. c), la normativa nazionale è vincolante anche per i trattamenti effettuati da responsabili non stabiliti nell'Unione Europea mediante strumenti situati sul territorio degli Stati membri.

Quindi, per le operazioni di trattamento in cui interviene un responsabile di un paese terzo, il criterio di collegamento con la normativa dello stato membro non è più il luogo di stabilimento del responsabile, bensì l'ubicazione territoriale degli strumenti utilizzati.

Inoltre, non è necessario che la persona oggetto di tutela della normativa sia un cittadino comunitario o sia fisicamente presente o residente nell'UE, la direttiva, infatti, armonizza le normative degli Stati membri in materia di diritti fondamentali riconosciuti a tutti gli esser umani.

Le disposizioni del titolo X del Codice in materia di protezione dei dati personali riguardo alle comunicazioni elettroniche sono direttamente collegate al suddetto quadro comunitario ed internazionale.

Come per la Direttiva n. 2002/58/ CE in relazione alla Direttiva generale n. 96/45/ CE, anche in questo caso quanto previsto dal titolo

[482] C. FILIPPI, *Le nuove regole per i servizi di comunicazione elettronica:l'attuazione della direttiva 2002/58. La tutela della riservatezza su internet e reti telematiche*, G. SANTANIELLO (in a cura di), La protezione dei dati personali, op. cit., pag 625; A. MANEGGIA, *La tutela della privacy nell'era delle comunicazioni elettroniche: cosa ha cambiato Internet?*, in In.Law, 2006, op cit.

specifico del Codice integra e non sostituisce quanto previsto nella parte generale. Pertanto, per tutto ciò che non risulta coperto dalle disposizioni sulle comunicazioni elettroniche e per i trattamenti non rientranti nell'ambito di applicazione dello stesso, vale la normativa generale del Codice.

In particolare, l'art 121 ha specificato che il capo X si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni, come definiti dall'art 4, secondo comma, dello stesso Codice.

L'art. 122 riguarda, invece, l'utilizzo di strumenti nell'ambito della rete, tramite i quali è possibile archiviare informazioni negli apparecchi terminali di abbonati o utenti, accedere alla informazioni registrate o monitorare le operazioni compiute dall'utente durante l'accesso alla rete. Al riguardo il Codice ha stabilito il divieto di realizzare le predette operazioni, prevedendo, tuttavia alcune eccezioni.

E' comunque richiesto che il fornitore abbia il consenso espresso dell'abbonato o dell'utente, ai quali deve essere fornita, a tal fine, una preventiva informativa dettagliata, dalla quale risultino sia gli elementi indicati dall'art 13 del Codice sia le finalità e la durata del trattamento.

Il Codice, inoltre, ha rinviato al Codice di deontologia previsto dall'art. 133, cui è stata demandata la specifica individuazione dei presupposti e dei limiti entro i quali è consentito l'uso dei predetti dispositivi.

Per quanto riguarda la disciplina dei dati relativi al traffico, l'art. 123 del Codice ha previsto che questi vengano cancellati o resi anonimi dal fornitore della rete o del servizio, quando si conclude la trasmissione della comunicazione, nell'ambito della quale erano stati trattati e memorizzati.

Accanto a tale previsione generale, lo stesso art. 123 ha individuato, poi, le ipotesi ed i limiti in cui è ammesso l'ulteriore trattamento dei dati relativi al traffico.

Sempre riguardo ai dati di traffico, l'art. 132 ne ha previsto, invece, la conservazione per dodici mesi per il traffico telematico (ventiquattro per quello telefonico) dalla data della comunicazione, ai fini di accertamento e repressione dei reati, esclusi comunque i contenuti delle comunicazioni.

I dai relativi all'ubicazione, diversi dai dati relativi al traffico, sono disciplinati dall'art 126 del Codice, secondo il quale possono essere trattati solo se anonimi o se l'utente o l'abbonato ha manifestato previamente il proprio consenso, revocabile in ogni momento, e nella misura e per la durata necessari per la fornitura del servizio a valore aggiunto richiesto.

Pure l'art. 130 del Codice, relativo alla comunicazioni pubblicitarie o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale, è incentrato sul consenso dell'interessato.

É vietato in ogni caso l'invio di comunicazioni per le suddette finalità o, comunque, a scopo promozionale, effettuato camuffando o celando l'identità del mittente o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui all'articolo 7 del Codice.

La disposizione prevista dall'art. 131 del Codice è volta, invece, a garantire specificatamente la riservatezza delle comunicazioni elettroniche. E' stato previsto, infatti, in capo ai diversi soggetti coinvolti a vario titolo nella comunicazione, l'obbligo di informare la controparte e/o gli interlocutori di qualunque tipo di situazione che permetta di far apprendere, in modo anche non intenzionale, il contenuto della comunicazione a soggetti diversi da quelli coinvolti nella comunicazione stessa.

L'art. 133 ha prescritto, come indicato, la predisposizione di un codice di deontologia e di buona condotta[483], riguardante i trattamenti dei dati personali effettuati dai fornitori di servizi di comunicazione e di informazione offerti nell'ambito di internet e delle reti telematiche.

Nella relativa disposizione si fa riferimento alla necessità di individuare i criteri volti ad "assicurare ed uniformare una più adeguata informazione e consapevolezza degli utenti delle reti di comunicazione elettronica gestite da soggetti pubblici e privati rispetto ai tipi di dati personali trattati e alle modalità del loro trattamento, in particolare attraverso informative fornite in linea in modo agevole e interattivo, per favorire una più ampia trasparenza e correttezza nei confronti dei medesimi utenti e il pieno rispetto dei principi di cui all'articolo 11 (…)".

[483] Cfr. art 12 del Codice, secondo il quale 1. Il Garante promuove nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività (…), la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, ne verifica la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto.

Al riguardo si osserva come, sebbene sia così tanto avvertita la necessità di regole specifiche relative alla tutela della privacy, tanto da sentire la necessità di un vero e proprio *Bill of rights* di internet, il suddetto codice di deontologia non è stato ancora approvato.

Questo probabilmente si deve, da una parte, alla difficoltà di riuscire a trovare un accordo nell'ambito delle categorie interessate, ma, forse soprattutto per la caratteristica spiccatamente globale di internet. Per essere un codice effettivamente efficace ed utile agli scopi dichiarati dovrebbe essere, infatti, espressione di principi riconosciuti ed applicati anche livello internazionale.

Infine, particolare rilevanza è stata data in generale agli aspetti concernenti la sicurezza dei dati oggetto di trattamento. È obbligatoria, infatti, l'adozione di idonee misure di sicurezza e nell'ambito di queste l'organizzazione, comunque, di misure minime di sicurezza che assicurino un livello, appunto minimo, di protezione dei dati personali.

Come verrà illustrato più avanti, per quanto riguarda il servizio di comunicazione elettronica accessibile al pubblico, l'obbligo di predisporre misure idonee è previsto dall'art. 32 del Codice, mentre le misure minime, relative al trattamento di dati personali effettuato con strumenti elettronici, sono disciplinate dall'art. 34 del Codice.

4.1.2. Anonimato protetto

Il soggetto che comunica in rete può avere interesse a rimanere anonimo, ad esempio, per partecipare a discussioni senza paura di essere stigmatizzato o discriminato oppure per denunciare abusi o, ancora, nell'ambito del commercio elettronico per avere la garanzia che i propri dati non vengano utilizzati a fini diversi dalla transazione conclusa e fatti circolare abusivamente. In generale, infatti, solo se gli utenti saranno sicuri dell'uso corretto dei loro dati si avvantaggeranno delle innovazioni tecnologiche.

Per questo motivo, diversi siti hanno trasformato la privacy in un vero e proprio asset concorrenziale del tipo: "se compri qui, i tuoi dati saranno distrutti molto prima degli altri".

La conservazione dei dati implica, infatti, il rischio, soprattutto fuori dall'Unione Europea, della rivendita a terzi, ad esempio per contatti promozionali [484], ma non è infrequente che anche lo Stato si avvalga delle informazioni contenute in data base commerciali di società private, aggirando le normative nazionali a tutela dei trattamento dei dati personali[485].

La dimensione della privacy non va considerata, tuttavia, soltanto da parte del soggetto attivo in rete, ma anche dal punto di vista dei soggetti che possono essere a loro volta oggetto della comunicazione in rete. Se, ad esempio, una persona viene diffamata su internet deve poter sapere chi è colui che ha commesso questo comportamento.

E' poi sicuramente necessario riuscire ad identificare chi compie reati tramite la rete, quali la pedofilia, la truffa ecc ecc.

Quindi, l'esigenza è di bilanciare la riservatezza dell'utente in rete che deve essere libero di poter manifestare il proprio pensiero, senza correre il rischio di essere per questo stigmatizzato, e dall'altra riuscire a garantire la possibilità di imputare ad un determinato soggetto la responsabilità di eventuali condotte illecite, attuate mediante l'uso di internet.

Già nel novembre 2008 il Consiglio d'Europa, a conclusione del 2987th Justice and Home Affairs Council meeting di Bruxelles, nelle sue conclusioni, relative ad una strategia di lavoro concertata e a misure pratiche di lotta alla criminalità informatica, ha evidenziato la necessità di superare la natura anonima dei servizi internet, per arrivare, attraverso un progetto congiunto, a una nuova forma di protezione dei diritti di ciascun cittadino: all'anonimato per chi naviga ed alla certezza della sanzione per chi subisce un danno dall'uso scorretto o illecito di internet[486].

---

[484] S. RODOTÀ, *Internet tra sicurezza e normalizzazione*, La Repubblica 15-1-2009, op. cit.

[485] Vedi ad esempio negli Stati Uniti il caso *Matrix* ovvero *Multistate Anti-Terrorism Information Exchange* del 2003. Si trattava del progetto di una banca dati preposta al fine di garantire la protezione del territorio nazionale. Per la creazione della banca dati ci si avvaleva delle informazioni messe a disposizione dai data base commerciali in deroga al Privacy Act del 1974. Le Agenzie federali hanno finito così per schedare indiscriminatamente i cittadini con dati relativi alla fedine penali, patenti, registrazioni veicoli, atti giudiziari, ecc fra le protese sempre più numerose di diverse associazioni, tra cui, in particolare, l'American Civil Liberties Union. Il progetto è stato abbandonato nel 2005. Cfr U. PAGALLO, *La Tutela della privacy nelgi Stati Uniti d'America e in Europa*, op cit., pag 102. Si veda anche il relativo dossier dell'American Civil Liberties Union, consultabile sul loro sito http://www.aclu.org/technology-and-liberty/feature-matrix.

[486] GUUE C62 del 17 marzo 2009, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:062:0016:0018:IT:PDF; Vedi M. KEYSER, *The Council of Europe Convention on Cybercrime*, consultabile su http://www.law.fsu.edu/Journals/transnational/vol12_2/keyser.pdf..

Una soluzione prospettata è stata quella del cd. anonimato protetto, attraverso il quale si garantisce a qualsiasi utente la possibilità di navigare in reste usando un nickname preferito, quindi, anche in modalità completamente anonima, purché abbia assolto all'obbligo di registrarsi tramite il provider utilizzando le proprie reali generalità, anche se nessuno può escludere che ci si registri con credenziali false.

Il provider, a sua volta, sarà obbligato a mettere a disposizione delle Autorità, legalmente autorizzate, i dati identificativi dell'utente quando sussistono le condizioni stabile sempre da una legge[487].

Esistono, però, programmi che garantiscono non solo l'anonimato dell'utente, ma anche la possibilità di accedere a siti bloccati; alcuni di questi programmi sono gratuiti altri a pagamento e molto spesso sono gestiti da società localizzate in Paesi stranieri[488].

In particolare, navigare anonimi significa mascherare l'indirizzo IP, ossia l'identificativo che viene assegnato al momento dell' accesso ad internet e che individua ogni utente in modo univoco, per tutto il tempo che rimane connesso.

Il programma *CyberGhost VPN 2010* consente, ad esempio, di navigare anonimi su internet, in modo tale che i siti che vengono visitati non conoscono l'indirizzo IP dell'utente, ma "vedono" quello dei server *CyberGhost* ed il provider internet, che ha assegnato al navigante un indirizzo IP, non può né conoscere né vedere i siti web che questo visita, i download effettuati, i collegamenti dei siti Web visti e le informazioni scambiate, dal momento che la connessione ai server *CyberGhost* è criptata a 128 bit attraverso un collegamento VPN (rete privata virtuale). Da parte sua, la società proprietaria del programma assicura di non archiviare i dati relativi al traffico e di non divulgarli a terzi[489].

---

[487] S. MELE, *Privacy e user generated content (UGC)*, in L BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, op cit, pag 60; L. BOLOGNINI e P. PAGANINI, *La libertà di Internet e reati: sì all'anonimato protetto*, op. cit. consultabile su http://mediablog.corriere.it/2009/12/liberta_di_internet_e_reati_si.html.

[488] Per un elenco di 20 programmi che offrono questo servizio si veda http://www.bloginmano.com/2010/09/20-servizi-vpn-gratuiti-per-navigare-in.html; cfr anche Navigare anonimi su internet con i proxy, vpn e indirizzi Ip falsi, consultabile su http://www.navigaweb.net/2008/04/navigare-restando-anonimi-e-scaricare.html.

[489] http://www.towerlight2002.net/2010/07/31/navigare-anonimi-con-cyberghost-vpn-2010-basic-o-premium-gratis-per-un-anno/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3°+towerlight2002dotorg+%28Notizie+e+curiosita+da+internet%29.

4.1.3. Responsabilità del provider, misure minime di sicurezza e documento programmatico di sicurezza

Questi argomenti pongono anche la questione della responsabilità dei providers. Se l'intermediario tecnico, infatti, diventa anche l'intermediario giuridico, in quanto responsabile delle azioni compiute da terzi-anonimi, immessi da loro nella rete, il provider, per ovvie ragioni di autotutela, selezionerà in modo molto rigoroso chi potrà accedere alla rete e chi no, con il rischio di avviare di processi di censura e di fare dei providers una sorta di censori istituzionali[490]

La materia della responsabilità del provider è disciplinata dal D.lgs. 9 aprile 2003 n. 70, emanato in applicazione della direttiva 2000/31/CE.

In particolare, la questione della responsabilità degli ISP (*Internet Service Provider*) è affrontata negli articoli da 14 a 17, laddove sono distinte e tipizzate le attività caratteristiche del prestatore di servizi in esame, distinguendo le attività di "*mere conduit*", di "*caching*", di "*hosting*" e prevedendo per ciascuna di esse un regime differenziato di responsabilità[491].

Così, nell'attività di semplice trasporto delle informazioni generate da un utente del servizio (*mere conduit*), cioè per il semplice fatto di fornire il semplice accesso alla rete, il provider non può essere considerato responsabile dei dati trasmessi a meno che non dia origine egli stesso alla trasmissione, oppure non provveda alla selezione del destinatario della comunicazione, oppure non svolga un'attività volta alla selezione o all'alterazione delle informazioni trasmesse[492].

Nelle attività di memorizzazione (*chaching*) automatica, intermedia e temporanea delle informazioni originate dal fruitore, invece, si deve ritenere esente da ogni responsabilità il prestatore che non modifichi quei dati e che provveda, inoltre, a conformarsi alle condizioni di accesso, alle

[490] S. RODOTÀ, *Internet tra sicurezza e normalizzazione*, La Repubblica 15-1-2009, op. cit.

[491] Per una ricostruzione della responsabilità del provider e per l'applicazione della nuova disciplina si veda Sentenza 29 giugno 2004 n.2286/2004, Tribunale di Catania - Sezione Quarta Civile, www.altalex.com/index.php?idstr=30&idnot=7548; S. MELE, *Privacy e user generated content (UGC)*, in L BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, op cit, pag 55 e ss; M. GAMBULI, *La responsabilità penale dei provider per i reati commessi in internet*, www.altalex.com/index.php?idstr=0&idnot=9965.

[492] Art. n. 14 D.lgs. n.70/2003 cit.

informazioni e alle loro norme di aggiornamento convenute con le imprese di settore.

Allo stesso modo, deve essere ritenuto non responsabile tutte le volte che in cui agisca prontamente per rimuovere le informazioni memorizzate o disabilitarne l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente in rete o che l'accesso sia stato disabilitato, oppure ne sia stata disposta da un'autorità amministrativa o giurisdizionale la rimozione o la disabilitazione[493].

Infine, quando la prestazione del servizio consiste nella memorizzazione non automatica, intermedia e temporanea di informazioni fornite dall'utente del sistema (*hosting*), il prestatore non è responsabile a condizione non sia concretamente consapevole del fatto che l'attività o l'informazione è illecita e, per quanto riguarda le azioni risarcitorie, non sia al corrente di fatti o circostanze che rendano manifesta l'illiceità dell'attività o dell'informazione[494].

In ogni caso, pur non essendo ravvisabile in capo al provider un obbligo generico di sorveglianza sulle informazioni che trasmette e memorizza, né un obbligo di ricerca attiva di fatti illeciti sui propri sistemi, non appena venga a conoscenza di tali fatti, il prestatore deve agire prontamente per rimuovere le informazioni o per disabilitare l'accesso ai suoi servizi, avvertire le autorità competenti e mettere a disposizione delle stesse le informazioni richieste, pena il coinvolgimento nella responsabilità civile[495].

La sicurezza dei dati in rete, quindi, riveste notevole importanza. Come evidenziato nel paragrafo relativo al quadro giuridico di riferimento, il legislatore ha fatto obbligo di predisporre misure finalizzate a garantire, appunto, la sicurezza del trattamento dei dai personali nelle comunicazioni elettroniche, internet incluso.

493 Art. n. 15 D.lgs. n. 70/2003 cit.

494 Art. n. 16 D.lgs. n. 70/2003 cit.

495 Art. 17 D.lgs. n. 70/2003 cit. Vedi però la famosa sentenza n. 1972 del 24 febbraio 2010 emessa dal Tribunale di Milano, con cui il giudice Osca Magi ha condannato tre dirigenti di Google per aver violato la normativa sulla privacy in relazione alla diffusione in rete da pare di alcuni ragazzi di un video in cui un disabile subiva atti di bullismo "L'informativa sulla privacy", scrive il giudice Magi, "era del tutto carente o comunque talmente nascosta nelle condizioni generali del contratto da risultare assolutamente inefficace per i fini previsti dalla legge". La condanna dei dirigenti di Google, infatti, secondo il magistrato, "non viene qui costruita sulla base di un obbligo preventivo di controllo sui dati immessi", ma per "un insufficiente (e colpevole) comunicazione degli obblighi di legge", riguardo l'informativa sulla privacy. La sentenza è consultabile su http://speciali.espresso.repubblica.it//pdf/Motivazioni_sentenza_Google.pdf.

Il Codice ha mantenuto la precedente distinzione tra misure di sicurezza minime ed idonee[496]. Le prime sono intese come il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto, riguardo ai rischi di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito e non conforme alle finalità della raccolta.

Le seconde sono realizzate tenendo conto delle conoscenze acquisite in base al progresso tecnico, alla natura delle informazioni e alle specifiche caratteristiche del trattamento.

La natura dinamica della disciplina della sicurezza si evidenzia anche nell'art 36 del Codice, in cui è stato previsto un aggiornamento periodico del disciplinare tecnico (allegato B del Codice), contenente le misure minime di sicurezza, "con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie e il Ministro per la semplificazione normativa, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore".

Due distinti regimi di responsabilità sono stati adottati dal Codice nel caso di violazione delle misure minime o delle misure idonee, assegnando alla prime una rilevanza penale[497] ed alle seconde una rilevanza essenzialmente civilista, con valutazioni da compiere in concreto e tenuto conto dello stadio di progresso tecnologico raggiunto e delle soluzioni disponibili.

Riguardo alle misure minime poi si è assistito, coerentemente alle caratteristiche già evidenziate del Codice, ad un processo di semplificazione rispetto alla normativa precedente nonché alla ricezione di regole tecniche altamente specialistiche, quali la disciplina ISO/IEC 17799 , le Linee Guida dell'OCSE[498] e la Direttiva n. 2002/58/CE.

---

[496] Cfr Titolo V – Sicurezza dei dati e dei sistemi- capo I Misure di sicurezza e capo II Misure minime di sicurezza del D.lgs. n. 196/2003, cit. Per quanto riguarda, in particolare, i servizi di comunicazione elettronica e i trattamenti con strumenti elettronici, si veda artt. 32 e 34 ed il disciplinare tecnico, allegato B del codice.. Cfr A. PARISI, *Sicurezza informatica e tutela della privacy*, Istituto Poligrafico Zecca dello Stato S.p.a., 2006 pag. 113 e ss; P. PERRI, *Privacy, diritto e sicurezza informatica*, Giuffrè, Milano 2007, pag. 195 e ss.

[497] Art. n. 169 D.lgs. n.196/2003.

[498] Disciplina ISO/IEC 17799, consultabile su http://www.iso.org/iso/catalogue_detail?csnumber=33441 e Raccomandazione del Consiglio OCSE/OECD relativa alla Linee guida per la sicurezza dei sistemi informativi e delle reti: verso una cultura della sicurezza, cit.

Inoltre la sicurezza è stata individuata dal Codice soprattutto in termini di progettualità. Si tende, così, a puntare sulla formazione dei responsabili ed incaricati del trattamento e sulla predisposizione di apposite politiche di comportamento, da revisionare con cadenza periodica.

Ancora, in tema di trattamenti elettronici, è stato introdotto il sistema di autenticazione informatica che ha precisato in modo analitico quanto già stabilito dalla precedente normativa, relativamente all'assegnazione di una password personale agli incaricati al trattamento per l'accesso al proprio pc.

La nuova disciplina ha stabilito che i suddetti incaricati devono essere dotati di credenziali di autenticazione (un codice associato ad una parola chiave) di carattere riservato, composte da almeno 8 caratteri.

Il titolare o il responsabile devono impartire adeguate istruzioni agli incaricati per non lasciare incustodito e accessibile l'elaboratore elettronico, durante una sessione di trattamento.

Tra le misure di sicurezza va segnalata, poi, l'utilizzazione di un sistema di autorizzazione per gli incaricati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Il nuovo Codice, inoltre, ha dedicato ampio spazio all'obbligo di predisporre il Documento Programmatico sulla Sicurezza (DPS)[499], che dove essere adottato entro il 31 marzo di ogni anno.

Tale dichiarazione deve contenere l'elenco dei trattamenti dei dati personali, la distribuzione dei compiti e delle responsabilità nella struttura, l'analisi dei rischi, le misure da adottare per garantire l'integrazione, l'integrità e la disponibilità dei dati, la protezione delle aree e dei locali.

---

[499] Il Documento Programmatico sulla Sicurezza è stato introdotto nel nostro ordinamento dall'art. 6 del D.P.R. 318/99 e ribadito, come visto, dall'art. 34 lett. g del D.lgs. n. 196/2003, anche se consiste in uno strumento utilizzato da diverso tempo dal management aziendale in generale. Con l'adozione del Codice della privacy ne è stato ampliato l'ambito di operatività, prevedendone l'adozione da parte di tutti coloro che fanno uso di strumenti elettronici per il trattamento dei dati personali sensibili e/o giudiziari, a prescindere dal fatto che siano accessibili mediate reti telematiche, come previsto in precedenza. Ha sollevato problemi interpretativi la formulazione dell'art. 34, la quale fa riferimento, per la predisposizione del D.P.S, al trattamento di dati personali effettuato con strumenti elettronici tout court. Il punto 19 dell'allegato B (disciplinare tecnico) indica, invece, il solo trattamento dei dati sensibili o giudiziari. E' stato necessario, quindi, l'intervento interpretativo del Garante, il quale ha specificato che l'art 34, adoperando l'espressione "nei modi previsti dal disciplinare tecnico", rinvia espressamente al contenuto dell'Allegato B), il quale, pertanto, può anche restringere l'ambito di applicazione della norma generale. Cfr. P. TROIANO, *Le misure di sicurezza*, in G. SANTANIELLO (a cura di), op. cit. pag. 209 e ss.; Il Parere del Garante del 22 marzo 2004, "Obblighi di sicurezza e documento programmatico: al 30 giugno la redazione del "dps"", consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=771307 e la Guida operativa per redigere il Documento programmatico sulla sicurezza (Dps), consultabile su http://www.garanteprivacy.it/garante/document?ID=1007740; A. PARISI, Sicurezza informatica e tutela della privacy, op. cit., pag. 121 e ss; P. PERRI, Privacy, diritto e sicurezza informatica, op. cit., pag. 249 e ss

Elemento particolarmente importante è la previsione espressa, in tale documento, di interventi formativi a favore degli incaricati al trattamento; tali interventi devono essere programmati già al momento dell'entrata in servizio del soggetto e ripetuti in caso di cambio di mansione.

Il legislatore ha attribuito grande valore alla realizzazione di questo adempimento, prevedendo che della sua adozione così come del suo aggiornamento il titolare debba riferire nella relazione accompagnatoria del bilancio d'esercizio, se dovuta.

Il titolare, inoltre, oltre ad essere tenuto ad adottare idonei programmi antivirus, ha il compito di impartire istruzioni organizzative e tecniche che prevedano il salvataggio dei dati con frequenza almeno settimanale. In tema di *disaster recovery*,[500] il titolare e il responsabile devono adottare idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi compatibili con i diritti degli interessati e non superiori a sette giorni.

Il titolare che si avvale di soggetti esterni per le misure minime di sicurezza (c.d. *outsourcing*) deve farsi rilasciare dall'installatore una descrizione scritta, c.d. attestato di conformità, dell'intervento effettuato, che ne attesta la corrispondenza alle disposizioni del suddetto disciplinare tecnico.

4.1.4. Furti d'identità

Si è visto come internet non si sottrae alle norme sulla protezione dei dati personali, anzi proprio per le sue caratteristiche strutturali da più parti è stata richiesta una disciplina specifica. Internet è uno spazio globale, in cui sempre più le persone sono in grado di produrre e scambiare contenuti.

Accanto all'identità reale oggi esiste un'identità elettronica virtuale (eID) che assume sempre maggiore rilevanza, come si è indicato, anche nei rapporti con le amministrazioni pubbliche nazionali ed internazionali, nel quadro dell' e-government.

[500] Per *Disaster Recovery* (brevemente DR) si intende l'insieme di misure tecnologiche atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business a fronte di gravi emergenze. Fonte Wikipedia.

Tuttavia, poiché identità elettronica ed identità reale possono non coincidere, nel mondo digitale una delle principali difficoltà consiste nell'essere certi che un soggetto sia effettivamente colui che si è qualificato; a questo, poi, devono poter essere ricondotti anche giuridicamente tutti gli effetti delle azioni poste in essere. La presenza di un soggetto sulla rete, in realtà, nella gran parte dei casi non consente di sapere con certezza se colui con il quale stiamo interagendo sia veramente chi dichiara di essere.

Particolare rilevanza assume al riguardo il rischio di furto d'identità.

Anche se i dati personali possono essere sottratti in molti modi sia dentro sia fuori internet, è comunque possibile individuare alcune delle tecniche utilizzate più frequentemente.

Fra queste rientra l'appropriazione dell'*hard disk* del computer, ad esempio, al momento della vendita del proprio pc. Infatti, sebbene i dati siano stati cancellati, è difficile che siano stati in realtà rimossi completamente dai supporti in maniera definitiva e che attraverso particolari tool[501] non sia possibile recuperare, quindi, anche solo parte delle informazioni salvate in precedenza.

Un altro metodo consiste nell'utilizzo di un "software malevolo"(*malware-keylogger*) o dispositivi hardware che registrano tutto quello che viene digitato sulla tastiera (*keylogger*)[502]. Il *malware- keylogger* consiste in un virus come un *Trojan*[503] o *Worm*[504], che si può ricevere anche per posta elettronica.

Una volta nel pc, il software del virus consente l'installazione del *keylogger*[505] che inizia a sua volta a registrare tutto quello che viene digitato sulla tastiera. Come indicato, il *keylogger* può anche consistere in un dispositivo che viene collegato al pc e da questo acquisisce informazioni.

---

[501] Nel linguaggio informatico si tratta di una applicazione o programma che svolge un determinato compito.

[502] Cfr. N. FABIANO, *La lotta ai furti di identità nel Web 2.0*, in L BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, op cit., pag. 68 e ss.

[503] Detti anche Cavalli di Troia per descrivere la loro funzione, i *troian* sono programmi che si presentano con funzionalità apparentemente innocue, ma che in realtà compiono attività nascoste, tra cui appunto carpire dati ed informazioni dell'utente. Cfr A. PARISI, *Sicurezza informatica e tutela della privacy*, op. cit., pag. 33 e ss.

[504] Il *worm* ha come obiettivo la moltiplicazione di se stesso all'interno di un ambiente di rete in più computer possibili, gli effetti dannosi sulle macchine sono in questo caso indiretti e non costituiscono lo scopo primario del software, al contrario dei virus in senso stretto che mirano a danneggiare le risorse di un elaboratore, siano esse fisiche (hardware) o logiche (dati, programmi ecc). Cfr A. PARISI, *Sicurezza informatica e tutela della privacy*, op. cit., pag. 36 e ss.

[505] A. PARISI, *Sicurezza informatica e tutela della privacy*, op. cit., pag. 76.

I dati personali, inoltre, possono essere sottratti mediante la tecnica del cd. *phishing*, fenomeno che desta particolare preoccupazione per il suo incremento negli ultimi anni.

La parola *phishing* deriva dall'unione delle parole inglesi "*password*", "*harvesting*" e "*fishing*". La frode viene realizzata attraverso l'invio di e-mail contraffatte con la grafica ed i loghi ufficiali di aziende, istituzioni e soprattutto istituti di credito, che invitano il destinatario a fornire informazioni, motivando tale richiesta con ragioni di natura tecnica.

Si segnalano, inoltre, i primi casi di *voice phishing* (*vhishing*) o *smishing*, l'utente riceve sul telefonino un sms dalla banca che lo invita rispondere per comunicare i propri dati personali oppure a chiamare un certo numero telefonico perché, ad esempio, la sua carta di credito è stata clonata.

L'utente, in giustificabile ansia, non controlla la corrispondenza del numero con quello indicato a suo tempo dalla banca, chiama e un risponditore identico a quello della banca risponde e chiede le credenziali per acceder ai servizi, ottenendo così tutte le informazioni per un accesso illegale al banking[506]

Un'altra tecnica utilizzata è quella nota come "*man in the middle*" (ossia uomo nel mezzo)[507] che può realizzarsi attraverso il dirottamento di una connessione (*connection hijacking*) della vittima verso un sito web, controllato da chi ha realizzato questa operazione, per poi sottrarre dati personali.

Inoltre, bisogna tenere presente che le risorse digitali ed informatiche consentono di effettuare banali ricerche su internet per conoscere i dati personali delle persone presenti in rete. Lo strumento utilizzato è un qualsiasi motore di ricerca (*Google, Yahoo*! *Bing* ecc.) oppure un blog, un forum o un social network.

Quest'ultimo in particolare è ormai un fenomeno diffusissimo a livello sociale, vedi per esempio *Facebook* o *Twitter*, e che per le sue implicazioni in termini di raccolta, gestione, trasferimento e trattamento di informazioni anche molto personali è sempre più oggetto di attenzione.

---

[506] R. BARESI, *La sicurezza informatica, una nuova sfida per il mondo bancario*, consultabile su http://www.01net.it/articoli/0,1254,1_ART_78205,00.html.

[507] Cfr. N. FABIANO, *La lotta ai furti di identità nel Web 2.0*, in L BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, op cit, pag. 77; A. PARISI, Sicurezza informatica e tutela della privacy, op. cit., pag. 77-78.

L'utente che generalmente si iscrive in un social network è motivato dalla volontà di condividere con altri idee, esperienze, contenuti ed accade molto frequentemente che sul proprio profilo si registrino numerosi dati personali, così come se ne condividano altrettanti.

I dati personali (anche attraverso foto e video), contenuti nel proprio profilo o comunque condivisi, possono raggiungere, se non vengono apposte limitazioni da parte dell'utente, anche l'intera comunità degli abbonati, che può essere formata anche da milioni di persone.

I social network sono vere e proprie "piazze virtuali", in cui i dati possono essere copiati da altri membri della rete o da terzi esterni e venire utilizzati per costruire profili personali o essere ripubblicati altrove.

Per questo motivo, le piattaforme di social network sono diventate molto invitanti da parte di chi ha interesse a sottrarre dati personali per finalità illecite[508].

Perciò, in occasione della 30° Conferenza internazionale delle Autorità di protezione dei dati, tenuta a Strasburgo il 17 ottobre 2008, 78 Autorità a tutela dei dati personali di diversi Sati hanno firmato una "Risoluzione sulla tutela della privacy nei servizi di social network"[509].

In essa sé stato evidenziato come i diversi social network, pur offrendo sicuramente nuove opportunità per la comunicazione, possano presentare rischi per la tutela della riservatezza sia degli utenti sia di terzi.

Le Autorità garanti hanno invitato, quindi, alla prudenza nell'uso dei servizi offerti, mentre i fornitori devono prevedere configurazioni tecniche idonee alla tutela della privacy ed adeguate misure di sicurezza.

Il 29 novembre 2009, il Garante italiano ha pubblicato una guida, "Social Network: Attenzione agli effetti collaterali"[510],al fine di aiutare gli utenti ad un uso consapevole del mezzo di comunicazione, illustrando i rischi ad esso connessi, in relazione alla tutela dei propri dati personali.

---

[508] Nella Relazione 2009 del Garante per la protezione dei dati personali è stato evidenziato, infatti, che: "In misura superiore rispetto all'anno precedente, nel 2009 sono pervenute segnalazioni con le quali si è lamentato il trattamento illecito dei dati personali su Facebook. Al riguardo si è ritenuto in via preliminare che, ove le immagini e le informazioni restino all'interno di un profilo o di un gruppo chiuso, il trattamento rientra tra quelli per fini esclusivamente personali, non destinati ad una comunicazione sistematica o alla diffusione, indicati all'art. 5, comma 3, del Codice, e perciò esclusi dall'applicazione della disciplina codicistica; qualora, invece, le informazioni siano visibili in rete in modo libero, e rinvenibili anche tramite i comuni motori di ricerca, poiché si tratta di diffusione, è da ritenersi applicabile integralmente il Codice", consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1730032.

[509] Consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1560428.

[510] Consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1614258.

Si tenga, inoltre, presente che in rete le informazioni tendono ad rimanere disponibili ed incancellabili. Infatti, spesso anche dopo aver cancellato il proprio profilo, i dati continuano a essere conservati nei server del social network, restando reperibili per decenni, senza che si possano "neutralizzare".

Questo avviene però anche fuori dai social network, normalmente grazie ai motori di ricerca che sono in grado di raccogliere e assemblare le notizie più disparate, comprese quelle molto datate, quelle non vere o che non corrispondono più alla realtà.

Qui si apre un'altra tematica connessa al trattamento dei dati personali in rete, ovvero quella riguardante il diritto all'oblio[511], alla cancellazione dei dati dopo un certo periodo, così come la questione generale dei *data retention*[512].

Si veda, ad esempio, la lettera scritta dal Garante italiano alla *Google* Inc. in America per far presente la situazione di soggetti italiani, danneggiati dal mantenimento di vecchie informazioni su pagine web non aggiornate, e della necessità di sollecitare comunque la collaborazione della società, "per individuare nel breve periodo soluzioni fattibili che permettano di garantire pienamente sul territorio italiano i diritti e le libertà fondamentali dei cittadini interessati, anche quando gli strumenti utilizzati per il trattamento non siano situati sul nostro territorio"[513].

Così come si segnala l'iniziativa nel dicembre 2008 da parte della *Microsoft* di portare a sei mesi il limite massimo di conservazione dei *logs*[514] del

---

511 Si vedano tre recenti decisioni del Garante in merito all'accoglimento delle opposizioni alla reperibilità delle proprie generalità attraverso i motori di ricerca (11 dicembre 2008 [doc. web n. 1583162], 11 dicembre 2008 [doc. web n. 1582866], 19 dicembre 2008 [doc. web n. 1583152]).

512 Per la disciplina della conservazione dei dati riferiti a comunicazioni elettroniche si rinvia all'art. 132 Codice in materia di protezione dei dati personali, al provvedimento generale del Garante del 17 gennaio 2008 (G.U. n. 30 del 5 febbraio 2008 e consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1482111) al provvedimento generale del Garante (G.U. n. 189 del 13 agosto 2008 e consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1538224) di parziale modifica del precedente a seguito della ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica, legge 18 marzo 2008, n. 48, al decreto legislativo 30 maggio 2008, n. 109, di recepimento della direttiva 2006/24/Ce nonché alle direttive 2002/58/Ce e n. 2006/24/Ce, già trattate nei precedenti paragrafi.

513 [doc. web n. 1339146] consultabile su www.garanteprivacy.it.

514 Il *logbook* (1800) era il registro di navigazione, presente in ogni nave, su cui veniva segnata, ad intervalli regolari la velocità, il tempo, la forza del vento, oltre a eventi significativi che accadevano durante la navigazione.

Con il significato di giornale di bordo, o semplicemente giornale, su cui vengono registrati gli eventi in ordine cronologico il termine è stato importato nell'informatica (1963) per indicare:

- la registrazione cronologica delle operazioni man mano che vengono eseguite
- il file su cui tali registrazioni sono memorizzate. Fonte Wikipedia

proprio motore di ricerca e di provvedere, una volta scaduto questo termine, alla completa anonimizzazione (non parziale, come invece proposto da altri operatori) dei dati di ricerca memorizzati sui propri server.

Il sistema garantisce non solamente la totale eliminazione dei numeri IP, ma anche la neutralizzazione dei *cookies*[515] e delle *query*[516] effettuate dall'utente. Spesso, infatti, da ciò che cerchiamo si può risalire con facilità alle nostre identità - si pensi al fenomeno dell'*egosurfing*[517] - e quindi fotografare con precisione chi siamo, con la creazione di un identikit virtuale[518].

Infine, in merito alla difficoltà di cancellare i propri dati personali presenti in rete, si segnala il proliferare di società definite "spazzini della rete"[519], con il compito appunto di ripulire internet da dati obsoleti o non graditi da parte dell'interessato.

Negli Stati Uniti ci sono società che propongono abbonamenti per una vita "senza incidenti virtuali". Ad esempio, per 15 dollari al mese la *Reputation Defender*[520] monitora il web e avverte i clienti di ogni nuovo commento o immagine che appare on line. Se c'è qualcosa di sgradito, viene "pulito". In Italia un servizio simile è offerto dalla *Reputation Manager*[521].

[515] I *cookie HTTP* (più comunemente denominati Web cookies, tracking cookies o semplicemente cookie) sono frammenti di testo inviati da un server ad un Web client (di solito un browser) e poi rimandati indietro dal client al server - senza subire modifiche - ogni volta che il client accede allo stesso server. I cookie HTTP sono usati per eseguire autenticazioni e tracciamento di sessioni e memorizzare informazioni specifiche riguardanti gli utenti che accedono al server, come ad esempio i siti preferiti o, in caso di acquisti on-line, il contenuto dei loro "carrelli della spesa" (shopping cart).Fonte Wikipedia. Cfr C. FILIPPI, *Le nuove regole per i servizi di comunicazione elettronica:l'attuazione della direttiva 2002/58. La tutela della riservatezza su internet e reti telematiche*, in La protezione dei dati personali , a cura di G. SANTANIELLO, op. cit., pagine 638-640.

[516] Il termine *query*, in informatica, viene utilizzato per indicare l'interrogazione di un database per cercare dati o informazioni. Fonte Wikipedia.

[517] Il termine *egosurfing* è utilizzato per descrivere l'atto di inserire il proprio nome in un motore di ricerca web al fine di valutare la propria presenza e rilevanza su Internet. Il termine, che deriva dall'inglese (to surf = navigare) e che è entrato nell'Oxford English Dictionary nel 1998, viene utilizzato anche nell'ambito della cultura Internet italiana. Inoltre con *egosurfing* si può indicare l'atto di valutare congiuntamente l'importanza del proprio nome e del proprio sito web o blog. Fonte Wikipedia.

[518] Cfr. www.istitutoitalianoprivacy.it.

[519] A. GINORI, *Gli spazzini del passato on line*, articolo pubblicato sul quotidiano La Repubblica, mercoledì 10 dicembre 2009.

[520] www.reputationdefender.com.

[521] www.reputazioneonline.it.

4.1.5. Lo spam

Altro fenomeno legato alla questione del rapporto fra internet e privacy è il fenomeno dello *spamming*[522].

Lo *spamming* è l'invio non sollecitato, ripetuto ed indiscriminato, soprattutto tramite e-mail, di messaggi pubblicitari e promozionali che permette di raggiungere un numero elevato di utenti internet. La fattispecie si distingue, altresì, per il fatto che generalmente il mittente non è riconoscibile, nonché per l'assenza di un'opzione di *opt-out* che consente a chi riceve un messaggio di cancellare le proprie coordinate elettroniche dalla liste di invio del mittente.

In questo caso è necessario operare un bilanciamento fra diritto alla privacy e diritto d'iniziativa economica[523].

Qui la tutela della riservatezza, come tutela all'autodeterminazione informativa, riguarda sia il controllo sul trattamento dei dati personali sia il controllo sulle informazioni che entrano nella nostra sfera privata. La tutela avviene soprattutto attraverso lo strumento del consenso informato prestato mediante, ad esempio, la suddetta tecnica dell'*opt out* (art.130 D.lgs. n. 196/03[524]), con cui l'utente ha la possibilità di rifiutare tale utilizzo del

[522] Send phenomenal amounts of mail (Spam).

[523] G. CREA, *La protezione dei dati personali tra diritti d'impresa, dei consumatori, della concorrenza*, in L. BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, op cit, pag. 138 e ss.

[524] Art. 130. Comunicazioni indesiderate

1. L'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso dell'interessato.

2. La disposizione di cui al comma 1 si applica anche alle comunicazioni elettroniche, effettuate per le finalità ivi indicate, mediante posta elettronica, telefax, messaggi del tipo Mms (*Multimedia Messaging Service*) o Sms (*Short Message Service*) o di altro tipo.

3.Fuori dei casi di cui ai commi 1 e 2, ulteriori comunicazioni per le finalità di cui ai medesimi commi effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli 23 e 24 nonché ai sensi di quanto previsto dal comma 3-bis del presente articolo.

3-bis (omissis)

3-ter (omissis)

3-quater (omissis)

4. Fatto salvo quanto previsto nel comma 1, se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente comma, è informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente.

5. É vietato in ogni caso l'invio di comunicazioni per le finalità di cui al comma 1 o, comunque, a scopo promozionale, effettuato camuffando o celando l'identità del mittente o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui all'articolo 7.

proprio indirizzo e-mail, all'atto del conferimento del dato in esame oppure in un secondo momento.

Il fenomeno dello spamming in rete, detto anche "*junk e-mail*" (e-mail spazzatura), ha suscitato e suscita numerosi dibattiti ed interventi da parte del Garante a causa dei continui reclami e segnalazioni rivoltigli dai cittadini: fra questi, ad esempio, il Provvedimento Generale sullo spamming e sulle regole per un corretto invio delle e-mail pubblicitarie, del 29 maggio 2003[525], nel quale sono state dettate le regole per un corretto invio di e-mail pubblicitarie, quali, ad esempio, il divieto di invio anonimo di messaggi pubblicitari, il rispetto del consenso informato e della trasparenza.

Inoltre, dato che spesso i messaggi vengono dall'estero, il provvedimento ha previsto che il destinatario possa richiedere l'intervento delle autorità straniere preposte alla disciplina della privacy per le verifiche in merito alla leicità o meno del comportamento del mittente.

Con un comunicato stampa del 3 settembre 2003, inoltre, il Garante ha ribadito che lo spamming a fini di profitto costituisce reato[526].

In ambito internazionale, si segnala la partecipazione del Garante ai lavori del Cnsa[527] (*Contact Network of Spam Authorities*) che si tengono presso la Commissione europea- Direzione generale società dell'informazione e media, in vista della predisposizione di un documento comune, London Action Plan[528], per la definizione di procedure atte a facilitare le indagini sullo spam.

Bisogna sottolineare anche iniziative degli stessi providers e delle aziende volte a contenere il fenomeno dello *spamming*, inquadrando così la tutela

6. In caso di reiterata violazione delle disposizioni di cui al presente articolo il Garante può, provvedendo ai sensi dell'articolo 143, comma 1, lettera b), altresì prescrivere a fornitori di servizi di comunicazione elettronica di adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono stati inviate le comunicazioni.

525 Consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=29840 [doc. web n. 29840]; Si veda anche il provvedimento del Garante del 15 luglio 2010 relativo alla raccolta di dati tramite internet per finalità promozionali, per il quale è sempre necessario il consenso degli interessati specifico, libero e documentato per iscritto per ciascuna delle predette finalità, consultabile su http://www.garante.privacy.it/garante/doc.jsp?ID=1741998.

526 Comunicato stampa consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=272444. Intervento del Garante nel dicembre 2002 di cui il suddetto comunicato stampa era relativo al Multilevel Mlm cd "Catena di Sant'Antonio elettronica". Nel messaggio inviato era contenuto l'invito ad inserirsi in un meccanismo per l'invio sistematico di e-mail ad altri destinatari al fine di trarne profitti economici. La catena era stata attivata da un soggetto privato, il quale oppose al Garante l'utilizzo personale dei dati e quindi la non applicabilità della legge sulla privacy. Consultabile su www.gatanteprivacy.it.

527 Per un quadro delle iniziative e della normativa in ambito comunitario si veda http://ec.europa.eu/information_society/policy/ecomm/todays_framework/privacy_protection/spam/index_en.htm.

528 http://www.londonactionplan.com/.

della privacy dei consumatori non solo come un costo, ma anche come una risorsa per lo sviluppo del commercio in rete. Così, ad esempio, sono cresciuti gli investimenti in tecnologia *anti-spamming*, in informativa ed in attività di ricerca e di sviluppo di nuove strategie e sforzi da parte delle aziende per riuscire ad instaurare un trasparente rapporto con i consumatori, basato anche su e-mail con preventivo e selezionato consenso.

A questo, inoltre, si aggiunge anche la continua crescita informatica dell'utente in rete, sempre più accorto ed esigente.

Pertanto, guardando al fenomeno nel suo complesso, anche in quest'ambito sembra che un approccio multi-strategico al problema, ossia basato su interventi legislativi, auto-regolamentazione, tecnologia avanzata e cooperazione internazionale possa essere la soluzione migliore per ridurre l'uso distorto del mezzo tecnologico, mediante lo spamming[529].

4.1.6. Privacy by design e social engineering

Si è già indicato come un accento sempre più rilevante in materia di tutela dei dati personali nelle nuove tecnologie informatiche viene posto sulle cd. *privacy enhancing technologies* (PETs), ovvero sulle tecnologie stesse, in questo caso, a protezione della privacy.

Tuttavia, come è stato sottolineato, tra gli altri, da Herbert Bukert[530] il ricorso a queste tecnologie non è affatto neutrale, in quanto esse rappresentano pur sempre un tentativo di rispondere ad un problema politico e sociale. Ad esempio, le tecniche di filtraggio per tenere lontani i minori da siti che possono rappresentare un rischio oppure per limitare l'accesso a siti che manifestano violenza, discriminazioni razziali implicano un potere di classificazione dell'informazione, a cui corrisponde nel software un segnale per cui si viene esclusi dall'accesso a quel tipo di informazione.

---

[529] G. RASI, *Cosa cambiare per le attività produttive*, in G. RASI (a cura di), Privacy: da costo a risorsa, consultabile su www.garanteprivacy.it

[530] H. BURKERT, *Privacy Enhancing Technologies: Typology, Critique, Vision*, in P. E. AGRE and M. ROTENBERG (eds.) Technology and privacy: the new landscape, Cambridge Mass. MIT Press 1998, cap. IV, consultabile su http://cognet.mit.edu/library/books/mitpress/0262511010/cache/chpt4.pdf.

La prospettiva della privacy garantita da soluzioni informatiche, comunque, si è in questi anni ulteriormente ampliata di una nuova specificazione, denominata *Privacy by Design* (PbD), la quale implica lo sviluppo e l'implementazione di soluzioni tecniche rispettose a monte dei dai personali degli utenti e che consentono a questi ultimi di controllarli facilmente.

La *privacy by design* consta di tre esplicazioni: 1) sui sistemi IT; 2) sullo sviluppo di pratiche business responsabili; 3) sul design delle interfacce web e delle infrastrutture[531].

Un esempio di *privacy by design* è rinvenibile nel progetto P_3P (*Plataform for Privacy Preferences*) del Consorzio per il *World Wibe Web* (W_3C). P_3P è una piattaforma per le preferenze privacy in grado di riconoscere automaticamente i siti internet che si impegnano con privacy policy rispettose dei dati personali degli utenti[532].

Per rendere possibile questo è necessario che i siti in questione descrivano le rispettive policy in un linguaggio standard leggibile della piattaforma P_3P chiamato APPEL (*A P_3P Preference Exchange Language*).

Sulla *privacy by design*, come aspetto evolutivo della tutela dei dati personali, si è occupata anche al 32° Conferenza internazionale delle Autorità di protezione dati che si è tenuta a Gerusalemme dal 27 al 29 ottobre 2010[533].

Un altro fattore molto importante da considerare ai fini della sicurezza in rete è l'aspetto umano. La tutela del proprio diritto alla privacy ed al corretto trattamento dei propri dati personali, infatti, è affidata principalmente all'uso consapevole del mezzo ed alla propria prudenza.

---

[531] Così L. BOLOGNINI, D. FULCO, P. PAGANINI, L. SCUDIERO, *Cloud computing e protezione dei dati personali: privacy e web globale, rischi e risorse*, in L BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, op cit, pag 33.

[532] E' presente un icona accanto a ciascun sito che diventa verde se questo soddisfa gli standard di privacy, rossa se non li garantisce, gialla se il sito non fornisce alcuna informazione sulla sue politiche in tema di privacy.

[533] "The power of technology must be harnessed to protect and enhance privacy. High fences, tinted glass windows, and more recently hashing, anonymization and encryption algorithms are also important technologies. Privacy by Design, or "PbD" as it is commonly referred to, is an innovative approach that treats privacy as a fundamental requirement in the development and operation of an organization's information technology and business practices. Perhaps its most innovative feature lies in its "Positive-Sum" nature. Proactively building privacy in from the outset, as PbD requires, avoids the dated zero-sum, win/lose paradigm in which privacy is unnecessarily traded off in the pursuit of other objectives." Gli interventi relativi sono consultabili in inglese su http://www.privacyconference2010.org/plenary3.asp.

Nella relazione introduttiva di Mauro Paissan[534] alla Giornata Europea della protezione dei dati personali del 2009, si legge che l'unico vero antivirus siamo noi stessi, utenti più consapevoli dei rischi che possono derivare da un uso senza criterio della rete.

A tal proposito si richiama l'attenzione su una particolare metodologia di attacco alla privacy, fondata appunto sul fattore umano, la cd. "*social engineering*".

Questa tecnica si fonda sul principio che dietro ogni sistema di sicurezza è sempre presente un uomo ed è molto più semplice "bucare" la sicurezza di un cervello umano che quella di un computer[535].

Il fenomeno del *phishing*, di cui si è in precedenza scritto, è proprio uno degli esempi applicativi di *social engineering*: si sfrutta cioè l'inconsapevole complicità dell'utente inesperto (e spesso terrorizzato), per ottenere l'effetto di sottrarre dati personali o compromettere il sistema[536].

Pertanto, ancora una volta assume una rilevanza fondamentale sensibilizzare gli utenti, anche mediante specifici corsi di formazione, sui i rischi che possono derivare da un uso inappropriato dei computer e delle diverse applicazioni.

4.2. Tecnologia ubiquitous computing

Le reti senza cavi o wireless costituiscono oggi una realtà del progresso tecnologico, in particolare l'*ubiquitous computing* rappresenta una nuova frontiera dell'informatica nella quale i computer, grazie allo sviluppo della nanotecnologia, divengono così piccoli da poter essere immersi, integrati, in quasi tutti gli oggetti che ci circondano. Questi dispositivi hanno e avranno sempre maggiori capacità di computazione e comunicazione.

In particolare, volendo esemplificare, le caratteristiche dell'*ubiquitous computing* sono: la pervasività funzionale del computer nelle attività quotidiane; la pervasività spaziale, il poter interagire con il computer ovunque nella dimensione spaziale; la trasparenza, cioè l'inavvertibilità della

[534] Consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1585131.

[535] Cfr A. PARISI, *Sicurezza informatica e tutela della privacy*, Op. cit. pag 40 e ss e 74; V anche la guida realizzata da un gruppo di hacker chiamati Black Hats su www.balckhats.it/papers.

[536] Si veda per un approfondimento anche sulle più attuali tecniche di phishing il sito di Anti-phishing Italia www.anti-phishing.it.

presenza di questa tecnologia; la Web presence, vale a dire la possibilità di integrare il mondo virtuale con il mondo fisico. Si pensi, ad esempio, ad un palmare in grado di interagire con i sensori degli oggetti circostanti[537].

Gli ambiti applicativi possono essere diversi: dall'automazione domestica, al controllo dello spostamento di oggetti, a sistemi di rilevamento di mal funzionamenti o di prevenzione in situazioni critiche, alla medicina, alla sicurezza.

In ambito militare, un'applicazione è costituita dalla già citata *smart dust*, polvere intelligente, ovvero "micro-sensori che vengono sparsi sul terreno con elicotteri o aerei, ai fini di fornire una rete di comunicazioni tra le truppe in ambienti ostili e anche per raccogliere dati sul terreno circa la presenza di gas tossici, batteri, presenza di radioattività ed altro"[538].

Il modello di interazione fra i dispositivi è generalmente *peer-to-peer*, modello abbastanza diffuso fra i vari sistemi di *file sharing* (scambio dati) utilizzati su internet: ogni sensore riceve le richieste, fornisce i dati, se li ha, oppure propaga le richieste ai sensori vicini.

Diversi sono gli aspetti che richiedono un bilanciamento fra il diritto alla privacy e la tecnologia *ubiquitous computing.*

L'informatica combinata con l'utilizzo di nanotecnologie diventa, infatti, particolarmente invasiva, in quanto progettata per essere invisibile e *ubiqua*. L'utente, pertanto, può interagire con essa automaticamente ed essere tracciato a sua insaputa.

Inoltre, con l'utilizzo del modello *peer-to-peer* per accedere ai servizi bisogna condividere le proprie risorse personali con altri utenti e l'*ubiquitous computing* permette di raccogliere grandi quantità di informazioni, che possono essere messe in relazione reciproca fra i diversi sistemi. Questo consente di dedurre conoscenze che non sono presenti nei dati, ma che possono essere ricostruite correlando i dati raccolti.

E' evidente, quindi, che una prima forma di tutela della privacy consiste nel rispetto del principio di necessità, in altre parole non utilizzare i dati personali dell'utente, se non quelli strettamente necessari per portare a compimento il servizio richiesto e comunque con il consenso dell'utente.

[537] L. V. MANCINI, *L'era dell'ubiquitous computing*, in Innovazioni tecnologiche e privacy, consultabile su www.garanteprivacy.it.op. cit.

[538] L. V. MANCINI, *L'era dell'ubiquitous computing* ,op cit.

In secondo luogo, visti i diversi contesti applicativi è necessario, come già messo in evidenza, "relativizzare" la tecnologia, cioè coordinare la disciplina normativa alle esigenze di quella particolare applicazione[539].

4.2.1. La tecnologia Rfid

Le Rfid, *Radio Frequency Identification*, cioè le cd "etichette intelligenti", sono dei *tag*s (dispositivi elettronici) flessibili che sostituiscono i codici a barre con cui vengono classificati e si movimentano i prodotti industriali.

Questi dispositivi sono alimentati direttamente dalla radiazione elettromagnetica del fascio di lettura in radio frequenza e, a differenza dei codici a barre, non occorre effettuare alcuna lettura visiva, in quanto l'emittente (il lettore Rfid) e l'antenna presenti nell'etichetta comunicano per prossimità (senza contatto fisico), fino ad una distanza di circa 10 metri e fino a 200 etichette al secondo.

Il loro costo si aggira in ordine ai 5/10 centesimi di dollaro Usa, anche questo spiega la loro sempre maggiore diffusione nel mondo della grande distribuzione.

Inoltre, i codici a barre identificano soltanto categorie di oggetti, ad esempio, il sapone per piatti; mentre, le etichette Rfid permettono di identificare ogni singola confezione.

Occorre, poi, distinguere fra etichette attive e passive; esistono chip con microprocessori ed etichette prive di microchip, ovviamente le prime sono meno costose, le seconde, invece, hanno maggiori funzioni. Stesso discorso vale per le etichette dotate di microprocessori di sola lettura o di lettura/scrittura.

Sono evidenti, dunque, le potenzialità di questa tecnologia per quanto concerne la raccolta di dati, così come i risparmi conseguibili nel settore delle vendite.

Anche in questo caso le applicazioni possibili sono numerose: dalla gestione di un magazzino al monitoraggio di bagagli.

---

539 S. MONTELEONE, *Dal controllo della tecnologia al controllo sulla tecnologia: necessità di un approccio tecnico giuridico*, consultabile su *e*-privacy.winstonsmith.info/2007/atti/ep2007_Monteleone_controllo_tecnologia.ppt.

Inoltre, come precedentemente illustrato, dopo gli attacchi terroristici dell'11 settembre in diversi paesi si sono cominciati ad inserire dispositivi Rfid nei documenti di viaggio. Al riguardo si rimanda a quanto già osservato in tema di carte elettroniche, passaporto elettronico ed identificatore unico[540] nelle politiche di e-government.

In questi casi, comunque, sono evidenti, le connessioni che la tutela dei dati personali ha con la garanzia delle libertà fondamentali.

Altri esempi di utilizzo di "etichette intelligenti" sono quello della Banca Centrale Europea ed al progetto di inserire dispositivi Rfid nelle banconote in Euro, oppure al progetto "*Veripay*"[541], cioè la possibilità di farsi inserire dei chip sottocutanei al fine di effettuare pagamenti - senza necessità di utilizzare carte di alcun tipo – semplicemente passando per l'area casse.

Di ben altra utilità, invece, si sono rivelate queste tecnologie in un ospedale di Singapore, nel quale durante l'epidemia di Sars nel 2003, ha assegnato etichette Rfid a tutto il personale ed ai pazienti in modo da individuare i soggetti con i quali la persona infettata aveva avuto contatti così da reagire tempestivamente ed isolare tali soggetti, al manifestarsi di un nuovo caso di malattia.

Tra l'altro, si può venire a contatto con questi dispositivi senza esserne a conoscenza, poiché è possibile inserire le etichette su capi di abbigliamento o tessuti e, persino, lavarle in lavatrice. Al riguardo è stato simpaticamente, ma molto oculatamente, notata la possibilità che "entrando in un negozio d'abbigliamento la commessa vi apostrofi come segue: 'Bello il completo di Brioni che indossa, ma perché non indossa anche la biancheria intima coordinata?'. La presenza della biancheria intima è stata individuata grazie alla presenza di dispositivi Rfid"[542].

Si veda, poi, l'esempio della Benetton che negli Stati Uniti è stata costretta dall'iniziativa di un'associazione dei consumatori a cessare l'uso di etichette Rfid sui vestiti oppure, ancora, l'esempio della Gilette che addirittura associava web cam ai dispositivi, in modo da individuare l'acquirente nel supermercato.

---

[540] Paragrafo 3.3.2 Carte elettroniche.

[541] Cfr ad esempio www.veripay.co.nz della Nuova Zelanda ed il sito di Applied Digital Solutions, società che offre sistemi di chippatura sottopelle a scopi di identificazione e transattivi, http://www.digitalangel.com/.

[542] A. DIX, *Le tecniche Rfid*, in Innovazioni tecnologiche e privacy,op. cit.

Inoltre, bisogna anche evidenziare che se le etichette non vengono rimosse o disattivate all'uscita del negozio o supermercato rendono continuamente identificabili gli oggetti e, indirettamente, chi li indossa o possiede. E' qui che entra particolarmente in gioco la tutela della privacy.

Alcuni rivenditori ritengono che sia inopportuno disattivare questi dispositivi in quanto potrebbero essere utili per dimostrare che il cliente ha comprato quel prodotto in quell'esercizio e, quindi, sarebbe in realtà una forma di tutela dello stesso acquirente, nel caso il prodotto si dimostrasse difettoso.

E' stato, però, giustamente osservato che in questi casi bisogna chiedersi se sia realmente necessario questa operazione, per garantire l'esercizio dei diritti del consumatore, o non si possa ricorrere ad altre possibilità senza dover essere sottoposti ad un tracciamento permanente attraverso i dispositivi Rfid[543].

Quantomeno, quindi, dovrebbe essere garantito all'utente di un servizio o ad un consumatore la possibilità di scegliere se spegnere o meno il chip che invia le informazioni relative all'oggetto[544].

Da quanto brevemente esposto, emerge chiaramente come questa tecnologia sia particolarmente idonea, per le sue caratteristiche, ad esser invasiva ed invisibile.

Come tutelare, quindi, la privacy di chi ne viene anche inconsapevolmente in contatto? Una prima forma di tutela è rendere a livello tecnico i dispositivi in questione visibili, magari secondo standard riconosciuti a livello internazionale.

In secondo luogo, bisognerebbe appunto dare la possibilità agli interessati di correggere o cancellare i dati raccolti una volta usciti dal negozio - anche se resta comunque da verificare la liceità del monitoraggio all'interno dell'esercizio commerciale - e poi individuare un responsabile del trattamento dei dati.

Altra questione è poi se le etichette disattivate possano essere riattivate in un momento successivo o magari da terzi fuori dal negozio per i fini più diversi[545].

---

[543] A.DIX, *Le tecniche Rfid*, in Innovazioni tecnologiche e privacy, op. cit.

[544] N. FABIANO, *Internet of things: il fenomeno e le prospettive giuridiche*, in L. BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, op cit., pag.91.

Si tenga presente, inoltre, che la comunicazione che avviene fra etichetta e lettore deve essere considerata una telecomunicazione; pertanto, ad essa si applica innanzitutto il principio di riservatezza delle telecomunicazioni, che deve essere tutelato.

Alcuni hanno proposto la tecnica della cifratura, che tuttavia, sebbene possa essere il rimedio più immediato, implica però un aumento di costi, giustificabile in alcune applicazioni - ad esempio militare o di sicurezza - ma difficilmente immaginabile in contesti quotidiani.

Anche per questa tecnologia, in ogni caso, è necessario insistere sul principio di necessità e proporzionalità, quindi prima di introdurre un dispositivo che raccoglie informazioni in modo automatico se ne deve verificare l'utilità effettiva in termini complessivi. Molte volte, infatti, non esiste alcuna necessità di raccogliere dati personali.

Negli Stati Uniti, alcuni Stati hanno già discusso ed adottato, almeno in parte, provvedimenti-quadro relativi all'utilizzazione di tecnologie Rfid e anche in questo caso c'è chi ha parlato di una vera e propria Carta dei Diritti per le Rfid[546].

Il *Center for Democracy and Technology* (Cdt)[547] ha elaborato, poi, una sorta di "decalogo" di buone prassi, per assicurare un utilizzo della tecnologia Rfid che sia rispettoso del diritto alla protezione della vita privata.

Al di là della questione dell'utilità pratica del moltiplicarsi di carte dei diritti per ogni tecnologia o applicazione di essa, sicuramente appare opportuno sviluppare un'adeguata disciplina tecnica e giuridica di riferimento, più condivisa possibile a livello internazionale, nel quadro di principi generali di tutela della dignità umana, di necessità e proporzionalità nel trattamento dei dati personali. Principi questi, peraltro, già presenti negli ordinamenti democratici sia nazionali che sopranazionali.

A questo proposito, nel 2005 il Garante per la protezione dei dati personali italiano ha individuato le garanzie per l'utilizzo delle etichette

[545] Rfid Tags Become Hacker Target, [Le etichette Rfid diventano bersagli per gli hacker], in http://news.com.com/2102-1029_3-5287912.html?tag/

[546] http://www.simson.net/clips/2002.TR.10.Rfid_Bill_Of_Rights.pdf; vedi anche CASPIAN, *The Rfid Right to Know Act of 2003*, all'indirizzo http://www.nocards.org/rfid/rfidbills.htm.l

[547] http://www.cdt.org. Il Cdt è un organismo no-profit che da molti anni segue, negli Usa, tematiche connesse alla tutela dei diritti civili. Il documento del Cdt si è concentrato soltanto sugli impieghi commerciali della tecnologia Rfid e non ha preso in considerazione altre possibili applicazioni (in particolare, nel campo dei rapporti di lavoro o per finalità specifiche di identificazione). Cfr. anche http://www.garanteprivacy.it/garante/doc.jsp?ID=1306421.

intelligenti nel rispetto dei principi generali stabiliti dal Codice in materia di protezione dei dati personali, e, in particolare, delle libertà, dei diritti fondamentali e della dignità degli interessati (art. 2, comma 1, del Codice). Principi che sono applicabili a prescindere dalla tecnologia utilizzata[548].

In particolare, il Garante ha richiesto il rigoroso rispetto dei principi di necessità (art. 3 del Codice), liceità (art 11 del Codice, comma 1, lett. a), finalità e qualità dei dati (art 11, comma 1, lett. b, c, d, e del Codice), proporzionalità (art. 11, comma 1, le d del Codice), informativa (art 13 del Codice), consenso (per il trattamento da parte di soggetti privati. Artt. 23 e ss. del Codice), esercizio dei diritti (artt. 7-10 del Codice).

Per quanto riguarda la rimozione e disattivazione delle etichette, è stato previsto che sia riconosciuta all'interessato la possibilità di ottenere, gratuitamente e in maniera agevole, la rimozione o la disattivazione delle etichette Rfid al momento dell'acquisto del prodotto, su cui è apposta l'etichetta, oppure al termine dell'utilizzo del dispositivo.

La crescente diffusione delle etichette Rfid , tra l'altro, ha poi spinto il Gruppo di lavoro Articolo 29 per la protezione dei dati personali ad appoggiare l'estensione ad alcuni dispositivi rfid della disciplina dettata dalla direttiva e-privacy, nel parere del 15 maggio 2008 sulla proposta da parte della Commissione europea di modifica della Direttiva sulle comunicazione elettroniche n. 2002/58/CE[549].

La stessa Commissione ha adottato il 12 maggio del 2009 una Raccomandazione[550] volta appunto a sollecitare un aggiornamento dei principi a tutela dei dati personali in considerazione dello sviluppo della tecnologia rfid. Sempre nel maggio del 2009 la Commissione ha aperto una consultazione pubblica, chiusa a dicembre 2009, sulla necessità di adeguamento del sistema normativo comunitario relativo alla tutela dei dati personali allo sviluppo della globalizzazione e all'uso di nuove tecnologie[551]

[548] Consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1109493.

[549] Il parere è consultabile su http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp150_it.pdf.

[550] Raccomandazione C(2009) 3200 final del 12 maggio 2009, consultabile in inglese su http://ec.europa.eu/ information_society/policy/rfid/documents/recommendationonrfid2009.pdf. Su questa si veda anche il parere del Gruppo ex art 29 n.5/2010 del 13 luglio 2010, consultabile in inglese su http://ec.europa.eu/justice/policies/privacy/ docs/wpdocs/2010/wp175_en.pdf.

[551] I risultati della consultazione pubblica sono riassunti in un documento del 4 novembre 2010 consultabile in inglese su http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf.

Infine, relativamente alla normativa applicabile alle tecnologie Rfid, il considerando 56 della già segnalata Direttiva n. 136/2009/CE, che modifica la Direttiva n. 58/2002/CE, ha precisato: "Il progresso tecnologico permette lo sviluppo di nuove applicazioni basate su dispositivi per la raccolta e l'identificazione dei dati, come ad esempio i dispositivi senza contatto che utilizzano le radiofrequenze. I RFID (Radio Frequency Identification Devices, dispositivi di identificazione a radiofrequenza), ad esempio, utilizzano le radiofrequenze per rilevare dati da etichette identificate in modo univoco, che possono in seguito essere trasferiti attraverso le reti di comunicazione esistenti.

Un ampio utilizzo di tali tecnologie può generare significativi vantaggi economici e sociali e, di conseguenza, apportare un contributo prezioso al mercato interno, sempre che il loro utilizzo risulti accettabile per la popolazione. A tal fine, è necessario garantire la tutela di tutti i diritti fondamentali degli individui, compreso il diritto alla vita privata e alla tutela dei dati a carattere personale.

Quando tali dispositivi sono collegati a reti di comunicazione elettronica accessibili al pubblico, o usano servizi di comunicazione elettronica come infrastruttura di base, è opportuno che si applichino le disposizioni pertinenti della direttiva 2002/58/CE (direttiva relativa alla vita privata e alle comunicazioni elettroniche), in particolare quelle sulla sicurezza, sui dati relativi al traffico e alla localizzazione e sulla riservatezza."[552].

4.2.2. La geolocalizzazione

La parola geolocalizzazione (o *geotagging* in inglese) è un esempio di parole entrate a far parte nel linguaggio comune come conseguenza del continuo sviluppo delle tecnologie.

In generale, con questo termine si indica il processo di abbinamento ad un documento (es. immagine fotografica, video, siti web ecc) di coordinate geografiche così da consentire di conoscere il posizionamento di persone od oggetti.

[552] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:01:IT:HTML.

La geolocalizzazione può avvenire sia inserendo manualmente i dati sia automaticamente, ad esempio attraverso un dispositivo dotato di collegamento satellitare GPS[553].

Le applicazioni pratiche rese possibili dai servizi di geolocalizzazione sono innumerevoli e spesso poco conosciute. Se non vi dubbio che questi servizi possono avere delle potenzialità di grande utilità sociale (si pensi alla possibilità di individuare persone in caso di terremoti o altri disastri naturali o soggetti scomparsi per altre cause oppure effettuare attività di controllo ambientale) è altrettanto evidente che questa tecnologia può avere anche una valenza negativa, in termini di possibile invasività della sfera, anche più riservata, dei cittadini[554].

Un esempio di questa pervasività sono i cellulari, oggetto ormai divenuto pressocchè indispensabile[555]. In essi i chip GPS per il posizionamento satellitare sono in effetti nelle dotazioni quasi standard, perciò, mandando ogni telefonino segnali ai satelliti, è possibile localizzare sempre più precisamente il suo possessore[556].

A questo riguardo, sono proliferati in questi ultimi anni i servizi di "*mobile tracking*". In Inghilterra, ad esempio, esiste il servizio *Follow us*[557], a cui si sono già iscritte oltre 200 mila persone, che consente di geolocalizzare il telefonino e, di conseguenza, il suo possessore.

Questo servizio si basa sul consenso dell'utente, il quale, registrandosi, accetta preventivamente i servizi ed attiva i servizi di mappatura del telefonino. Tuttavia, la prestazione del preventivo consenso non mette al sicuro da successive violazione della privacy, ad esempio, nel caso in cui il cellulare entri in possesso di un terzo malintenzionato. Bastano, infatti, pochi minuti, per registrarsi con la propria sim card, ricevere il primo sms che avverte l'attivazione del servizio, disattivare la notifica dei successi

[553] Il Global Positioning System (abbreviato in GPS, a sua volta abbreviazione di NAVSTAR GPS, acronimo di NAVigation Satellite Time And Ranging Global Positioning System), è un sistema di posizionamento su base satellitare, a copertura globale e continua. Fonte Wikipedia.

[554] A. DEL NINNO, *Geolocalizzazione: le sfide alla privacy nella società del controllo globale*, in L. BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, op cit., pag 97 e ss.

[555] Il tasso di penetrazione dei telefoni cellulari nel nostro Paese è uno dei più alti al mondo, pari circa all'86,4 %.

[556] Cfr R. STAGLIANO, *Silenzio, il cellulare ti spia. Se il telefonino diventa nemico*, La Repubblica, 2 luglio 2009, consultabile su http://www.repubblica.it/2009/07/sezioni/tecnologia/privacy-telefoni/privacy-telefoni/privacy-telefoni.html.

[557] www.followus.co.uk.

messaggi, per poter poi comodamente entrare nel sito del gestore e con pochi euro monitorare gli spostamenti dell'ignara vittima.

Fra gli altri esempi di applicazione di questa tecnologia, si segnala, inoltre, come da pochi mesi in Australia i genitori possono usare *MyMobileWatchdog*[558], un software sviluppato originariamente per la polizia americana. Una volta attivato, il servizio consente non solo la tracciatura del telefonino del minore, ma anche, attraverso un'applicazione web, di visionare tutti i contatti, i contenuti, gli sms/mms, le chiamate ricevute ed effettuate dal figlio.

Ancora, è stato segnalato che presto alcuni telefoni cellulari saranno dotati di chips Rfid, in cui saranno immagazzinate le generalità del titolare e altri dati identificativi. Tra i tanti usi possibili, viene fatto l'esempio del sistema di sicurezza contro utilizzi illeciti della propria carta di credito: se il proprietario del telefonino si trova in un posto diverso da quello dove avviene la transazione è probabile che la carta sia stata sottratta e, quindi, il sistema darà l'allarme. E' ovvio che in questo caso si tratta di un servizio utile all'utente.

Mettiamo però il caso che le stesse "etichette intelligenti" segnalino il soggetto all'interno di un grande magazzino[559] e a questo arrivino sms sulle promozioni disponibili. Se la pubblicità tramite cellulare dovesse seguire le previsioni di costante aumento, si comprendono bene le implicazioni negative in termini di invasività della privacy e di ricezione di informazioni non sollecitate. A queste dovrebbero, in ogni caso, applicarsi i principi già visti in tema di *spamming* e comunicazioni pubblicitarie, nonché quelli generali relativi al trattamento di dati personali[560].

Si vedano, ancora, i casi di due istituti scolastici americani che, fornendo ai propri studenti computer portatili muniti di webcam e di un particolare software, sono riusciti a monitorare di nascosto il loro comportamento.

---

[558] www.mymobilewatchdog.com.

[559] Ovvero all'interno di un POI o punto di interesse, incluso in una lista di posizioni ed indirizzi utili predeterminati per la creazione di servizi informativi di marketing.

[560] "Da tempo abbiamo verificato l'esistenza in commercio e anche su Internet di programmi che, una volta installati, consentono di localizzare costantemente l'apparecchio, rubarne i dati in esso contenuti e talvolta di ascoltare le conversazioni e leggere gli sms. In alcuni casi sono sistemi che possono avere usi "buoni", come consentire di rimanere in contatto durante un'escursione. Più spesso, però, no. L'uso di questi sistemi spia è e resta illecito e può dar luogo a gravi responsabilità penali". Programmi che "possono trasformare il cellulare in un delatore costante dei nostri comportamenti e quindi un nostro nemico" Franco Pizzetti, citato in R. STAGLIANO, *Silenzio, il cellulare ti spia. Se il telefonino diventa nemico*, La Repubblica, 2 luglio 2009, op cit.

La telecamera montata sul portatile, infatti, acquisiva le immagini e le trasmetteva all'istituto scolastico all'insaputa degli studenti e delle loro famiglie[561].

Di fronte a tali episodi è appena il caso di ricordare che, oltre alle norme previste dal Codice in materia di dati personali, l'interferenza illecita nella vita privata in Italia costituisce un reato, previsto dall'art. 615 bis del Codice penale[562].

Venendo, poi, al fenomeno già analizzato dei social network, uno degli ultimi sviluppi che sta interessando il *social networking* e il *community networking* riguarda proprio funzionalità legate alle tecnologie di geolocalizzazione.

In tal caso si parla di *geosocial networking*, per indicare la possibilità di caratterizzare le rete sociali sulla base della localizzazione degli utenti che ne fanno parte[563]. E' pur vero che in questi casi è richiesto il consenso preventivo del soggetto interessato, ma , com'è stato già evidenziato, questo non sempre può essere considerato una garanzia sufficiente.

Rischi analoghi per la privacy degli utenti derivano da un'applicazione intergrata del servizio *Google Maps*, chiamata *Latitudine*. Il suo funzionamento deriva dalla triangolazione GPS ed il cellulare: quest'ultimo trasmette la posizione a *Google* che fa comparire sulla mappa la nostra posizione. Il servizio *Latitudine* si integra poi con un altro denominato *Google Talk*, ovvero un servizio di *Voice over IP* (telefonate tramite internet) e di messaggistica istantanea.

Dal punto di vista della privacy, *Latidudine* è un servizio basato su consenso/autorizzazione preventivi alle diverse opzioni applicative,

---

561 Si veda l'art. di D. GELLES sul Financial Times, consultabile su http://www.ft.com/cms/s/2/aefb5d4e-1d97-11df-a893-00144feab49a.html e quello di L. M. FALCO, *Computer portatili agli studenti ma la scuola li spiava in casa*, su La Repubblica del 20 febbraio 2010, consultabile su http://www.repubblica.it/scuola/2010/02/20/news/scuola_usa_spia-2374378/ . Cfr anche http://www.informationsociety.it/ictlaw/tag/tecnologie-di-controllo.

562 Art. 615 bis – Interferenze illecite nella vita privata

1. Chiunque, mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614 [Violazione di domicilio, n.d.r.], e' punito con la reclusione da sei mesi a quattro anni.

2. Alla stessa pena soggiace, salvo che il fatto costituisca più grave reato, chi rivela o diffonde mediante qualsiasi mezzo d'informazione al pubblico le notizie o le immagini, ottenute nei modi indicati nella prima parte di questo articolo.

3. I delitti sono punibili a querela della persona offesa; tuttavia si procede d'ufficio e la pena e' della reclusione da uno a cinque anni se il fatto e' commesso da un pubblico ufficiale o ad un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione d'investigatore privato.

563 Cfr A. DEL NINNO, *Geolocalizzazione: le sfide alla privacy nella società del controllo globale*, in L. BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, op cit., pagg. 101-102.

modificabile in qualsiasi momento. Anche in questo caso, però, questo non garantisce la sicurezza nell'ipotesi, ad esempio, di illecita sottrazione del telefonino: l'eventuale ladro potrebbe disattivare la propria localizzazione, ma anche continuare a geolocalizzare i contatti del proprietario che aveva dato autorizzazione.

Inoltre, le informazioni di geolocalizzazione dell'utente del servizio *Latidudine* restano immagazzinate sul server di *Google*, almeno per quanto riguarda l'ultima posizione nota, con il rischio che un terzo ne venga a conoscenza per i fini più disparati, se non adeguatamente protette.

Altro servizio contenuto in *Google Maps* è il noto *Google Street View*, che permette di localizzare con altissima precisione le strade di numerose città del mondo. Questo ha sollevato critiche in ordine alla tutela della privacy, dovute al fatto che fosse possibile identificare le persone riprese nelle foto scattate da *Google.*

Al riguardo, il 25 ottobre 2010 il Garante della privacy è intervenuto con un provvedimento[564], con cui, pur ritenendo opportuna "la misura già adottata da *Google Inc.* di oscurare, prima della pubblicazione online, gli elementi che possono consentire un'identificazione diretta (ad esempio, i volti) o indiretta (ad esempio, le targhe dei veicoli) degli interessati", ha ritenuto necessario, comunque, che "gli interessati siano informati in modo idoneo ai sensi dell'art. 13 del Codice in relazione all'acquisizione di immagini da parte di Google Inc., affinché costoro possano scegliere di sottrarsi alla 'cattura' delle immagini, allontanandosi dal luogo oggetto di ripresa".

Le "*Google cars*"[565], quindi, dovranno essere facilmente individuabili, attraverso cartelli o adesivi ben visibili, che indichino in modo inequivocabile che si stanno acquisendo immagini fotografiche per il servizio *Street View.*

Alla società californiana è stato ordinato, inoltre, di pubblicare sul proprio sito web, tre giorni prima che inizino le riprese, le località visitate dalle vetture di *Street View.* Per le grandi città sarà necessario indicare i

[564] Consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1759972 . Il provvedimento è interessante anche perché viene applicata ad una società straniera la legge italiana a tutela dei dati personali, in quanto il trattamento è "effettuato mediante strumenti situati nel territorio dello Stato (art. 5 del Codice)"

[565] Le autovetture con installate le telecamere per le riprese delle strade.

quartieri in cui circoleranno le vetture. Analogo avviso dovrà essere pubblicato da *Google* sulle pagine di cronaca locale di almeno due quotidiani e diffuso per mezzo di un'emittente radiofonica locale per ogni regione visitata.

Alla società è stato anche imposto di nominare un proprio rappresentante sul territorio italiano, al quale possano rivolgersi i cittadini per la tutela dei loro diritti.

Per ogni inosservanza delle prescrizioni del Garante scatterà una sanzione amministrativa che potrà arrivare fino a centottantamila euro.

Da quanto brevemente esposto, ben si comprende come anche le tecnologie di geolocalizzazione siano, quindi, parte del quadro generale rappresentato dalla società globalizzata dell'informazione. Società, in cui diviene sempre più complesso padroneggiare la realtà in cui siamo immersi, assicurando a ciascuno il controllo sulla propria vita. "Mai come ora l'esplosione della tecnologia rende difficile una difesa effettiva ed efficace di questo diritto"[566].

5. Privacy e Tecnologie biometriche

Per biometria si intende il riconoscimento automatizzato di un soggetto o la verifica della sua identità sulla base di sue caratteristiche fisiche e comportamentali[567].

Le moderne tecniche biometriche si basano non solo sul riconoscimento delle impronte digitali, ma anche ad esempio, sulla geometria della mano, sulle caratteristiche dell'iride, del volto, della voce, sulla vascolarizzazione del dorso della mano o sulla modalità di apposizione della propria firma.

Un accorgimento tecnico in termini di tutela della privacy, con riferimento a questa, tecnologia è stato individuato nell'utilizzo del *template*, vale a dire del modello matematico della caratteristica fisica, invece dell'immagine della stessa. Dal *template*, infatti, è quasi impossibile ricostruire la caratteristica fisica di partenza.

[566] Relazione 2008 al Parlamento del Garante della privacy "Protezione dei dati e nuove tecnologie nel mondo in trasformazione" 2 luglio 2009, consultabile su www.garanteprivacy.it

[567] Cfr. G. PEIETRI, *Biometria e riconoscimento biometrico della persona*, consultabile su http://85.94.202.75/ sistemadocumentale/AreaDocumenti/E.../Biometria.doc

Un'altra accortezza è stata indicata nell'uso di processi di verifica di identità piuttosto che di identificazione: quest'ultimi necessitano di un archivio di dati biometrici, mentre la verifica di identità può avvenire anche senza di esso, magari inserendo le caratteristiche biometriche solo sul titolo in possesso dell'utente.

Il campo di applicazione delle tecniche biometriche è sia privato sia delle pubbliche amministrazioni.

In merito all'utilizzo di questi dispositivi ci si è chiesti se siano realmente necessari rispetto ai tradizionali metodi di identificazione, le risposte non posso che riferirsi alla singola applicazione, anche se sicuramente non devono essere sottovalutati i rischi di furto, smarrimento o clonazione dei titoli personali.

Questo introduce il problema della vulnerabilità di questa tecnologia, si veda il caso delle cd. "*gummy fingers*"[568]: una delle modalità di manipolazione delle impronte digitali.

Tuttavia, c'è chi ne rinviene un'indiscutibile utilità nel loro utilizzo: per esempio, nell'aeroporto di Amsterdam, un soggetto autenticato biometricamente può partire attraverso varchi separati, evitando file, grazie al programma Abc (*Automated Border Crossing*)[569]. Così come nell'aeroporto londinese di Heathrow, dove sono stati installati dei terminali con il sistema di riconoscimento dell'iride integrato nei lettori di card. I *frequent flyers* possono, quindi, volontariamente avvalersi della biometria per snellire le procedure di controllo e imbarco; la card contiene, infatti, tutti i dati contenuti nel passaporto.[570]

Si ricorda, inoltre, che attualmente negli Stati Uniti è attivo il progetto *Us Visit* (*United States Visitor and Immigrant Status Indicator Technology*) [571], il quale prevede che tutti i visitatori stranieri, all'atto di entrare negli Stati Uniti, lascino le proprie impronte digitali (oltre ad una fotografia del volto scattata dal funzionario dell'immigrazione). *Us Visit* non si applica ancora ai visitatori provenienti dai Paesi partecipanti al cosiddetto *Visa Waiver*

[568] Cfr. T. MATSUMOTO, H. MATSUMOTO, K. YAMADA, S. HOSHINO, *Impact of Artificial "Gummy" Fingers on Fingerprint Systems*, 2002, consultabile su http://cryptome.org/gummy.htm.

[569] M. SAVASTANO, *Recenti applicazioni biometriche*, in Innovazioni tecnologiche e privacy, op. cit.

[570] vedi www.biometriatech.com/dlarticolo.asp?id=1628.

[571] Vedi http://www.usembassy.it/visa/PassengerInformationCard-it.pdf.

Program[572] (i cui cittadini sono esentati dall'obbligo del visto per entrare negli Stati Uniti), tra cui l'Italia. Al riguardo, si pensa di estendere la raccolta delle impronte anche ai soggetti in uscita, in modo da poterle confrontare con quelle in entrata [573].

Anche in Europa sono previsti diversi progetti di implementazione delle tecnologie biometriche per il controllo delle frontiere nell'Unione Europea, si vedano, ad esempio, la Comunicazione del 2008 della Commissione europea EU1 ed il successivo documento tecnico di consultazione EU2[574].

In Italia solo alcuni Ministeri possono ancora permettersi questo tipo di tecnologia, gli aeroporti non hanno grandi mezzi e nel mercato privato le aziende hanno poche risorse da investire in questo settore, oltre ad esserci una certa reticenza verso il trattamento dei dati personali che ne consegue. Questa situazione ha spinto diverse aziende importatori o produttori di tecnologie biometriche a richiedere un intervento del Garante per la protezione dei dati personali, al fine di definire dei parametri di riferimento che, da una parte, tutelino il diritto alla privacy e, dall'altra, aprano il mercato all'utilizzo di queste tecnologie, usate in modo "sicuro".[575]

La stessa Autorità è intervenuta diverse volte sull'argomento e, tra l'altro, con deliberazione n. 53 del 2006 [576], ha dettato le "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati", le quali al paragrafo 4 si occupano di "dati biometrici e accesso ad 'aree riservate'".

In particolare, si legge che "l'uso generalizzato e incontrollato di dati biometrici, specie se ricavati dalle impronte digitali, non è lecito. Tali dati, per la loro peculiare natura, richiedono l'adozione di elevate cautele per prevenire possibili pregiudizi a danno degli interessati, con particolare riguardo a condotte illecite che determinino l'abusiva 'ricostruzione'

[572] Cfr http://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_traveler_guide_italian.pdf.

[573] Con tutte le conseguenti questioni anche in ordine alla gestione dei "visitatori" degli Stati Uniti le cui impronte all'uscita non coincideranno con quelle raccolte all'ingresso, in quanto in materia di riconoscimento delle impronte digitali, esistono ancora alte percentuali di errore. Vedi M. SAVIANO, *Recenti applicazioni biometriche*, in Innovazioni tecnologiche e privacy, op cit.

[574] Per un quadro dei progetti in corso e quelli previsti a livello europeo e la situazione a livello nazionale si rinvia al documenti del CNIPA http://www.cnipa.gov.it/html/docs/BIOMETRIA%20E%20SICUREZZA%20_DELLE%20FRONTIERE.pdf ed il documento presentato i n occasione dell'edizione 2009 del Forum PA il CNIPA http://www.cnipa.gov.it/html/docs/documenti%20biometrici%20sicurezza%20territorio%20frontiere.pdf.

[575] M. SAVASTANO, *Recenti applicazioni biometriche*, in Innovazioni tecnologiche e privacy, op. cit.

[576] Consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1364939.

dell'impronta - partendo dal modello di riferimento - e la sua ulteriore 'utilizzazione' a loro insaputa".

Nei casi in cui ne è consentita l'utilizzazione, inoltre, i sistemi informativi devono essere comunque "configurati in modo da ridurre al minimo l'utilizzazione di dati personali e da escluderne il trattamento, quando le finalità perseguite possono essere realizzate con modalità tali da permettere di identificare l'interessato solo in caso di necessità (artt. 3 e 11 del Codice)".

E' stato poi ritenuto adeguato e sufficiente l'utilizzo del "modello cifrato, su un supporto posto nell'esclusiva disponibilità dell'interessato (una *smart card* o un dispositivo analogo) e privo di indicazioni nominative riferibili a quest'ultimo (essendo sufficiente attribuire a ciascun dipendente un codice individuale)".

Infine, è stato previsto l'obbligo del previo consenso dell'interessato, il controllo dell'accesso ai dati raccolti solo da personale autorizzato e per le finalità previste. Il tempo di conservazione dei dati è stato indicato in media in 7 giorni e, in ogni caso, deve essere prevista la cancellazione automatica degli stessi[577].

Nella Pubblica Amministrazione italiana esistono iniziative che permettono di utilizzare soluzioni biometriche, ad esempio l'impronta digitale, quali la carta d'identità elettronica, il passaporto elettronico, la previsione del permesso di soggiorno elettronico per gli immigrati, la carta multi servizi della difesa, altre come l'Afis[578] per l'identificazione delle persone sospette o dei pregiudicati.

Il Cnipa (ora DigitPA[579]) ha realizzato un centro di competenza specifico per poter coordinare questa area della biometria, sia a favore delle pubbliche amministrazioni centrali che di quelle locali.

---

[577] Si segnalano, inoltre gli interventi del Garante: sul trattamento di dati biometrici in banca: 23 gennaio 2008 [doc. web n. 1490382, 1490463, 1490477, 1490533]; sulla rilevazione di impronte digitali ed immagini per accedere agli istituti di credito: limiti e garanzie 27 ottobre 2005 [doc. web n. 1246675]; Dati biometrici: vietati per la rilevazione dell'orario di lavoro: 2 ottobre 2008 [doc web. n. 1571502].

[578] Vedi http://it.wikipedia.org/wiki/AFIS_(informatica) e S. MARASCIO, *le impronte digitali ed il sistema Afis*, in http://www.criminiseriali.it/AFIS.pdf.

[579] Al cui interno è previsto ora un Ufficio Divisionale Tecnologie Innovative, il quale svolge un ruolo propositivo nei confronti della Pubblica Amministrazione verificando le esigenze di nuovi servizi o piattaforme tecnologiche avanzate e sperimentando soluzioni innovative. A tale scopo la struttura mantiene attivi sia i rapporti con le Università e Centri di Ricerca che con le maggiori imprese operanti nel settore dell'innovazione. L'ufficio è strutturato in due divisioni: Realtà virtuale e Laboratorio sperimentale. Quest'ultimo, in particolare, offre supporto all'Ente ed alle Pubbliche Amministrazioni nella realizzazione

Il gruppo di lavoro allora predisposto nel 2004 ha realizzato delle linee guida, in merito alle applicazioni biometriche nelle pubbliche amministrazioni. Il documento è stato redatto anche con l'ausilio di soggetti esterni, come ricercatori o personale accademico, rappresentanti dei Ministeri dell'interno, della giustizia e della difesa, le associazioni di fornitori di tecnologie di comunicazioni e informatica, nonché, in veste di uditore, di un rappresentante del Garante per la protezione dei dati personali.

I contenuti di queste linee guida sono: gli obiettivi, il processo biometrico e la sua descrizione, le diverse soluzioni che oggi esistono sul mercato e le applicazioni relative nei vari Paesi del mondo, le normative di riferimento, dove previste, e i livelli di sicurezza[580].

Nel 2007 il Garante per la protezione dei dai personali ha emanato un provvedimento generale recante "Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico"[581], nel quale, in riferimento all'utilizzo delle impronte digitali per la rilevazione dell'orario di lavoro ed in taluni casi a garantire speciali livelli di sicurezza, si è ribadita la necessità che tale utilizzo sia effettuato nel pieno rispetto della disciplina in materia di protezione dei dati personali.

In particolare, "il principio di necessità impone a ciascuna amministrazione titolare del trattamento di accertare se la finalità perseguita possa essere realizzata senza dati biometrici o evitando ogni eccesso nel loro utilizzo che ne comporti un trattamento sproporzionato (artt. 3 e 11 del Codice). Devono essere quindi valutati preventivamente altri sistemi, dispositivi e misure di sicurezza fisiche e logicistiche che possano assicurare una puntuale e attendibile verifica delle presenze e degli ingressi sul luogo di lavoro.

(…) Di regola, sistemi di rilevazione di impronte digitali nel luogo di lavoro possono essere quindi attivati soltanto per particolari esigenze di controllo dell'accesso a speciali aree dei luoghi di lavoro in cui si debbano

di attività sperimentali e ricerche finalizzate ad indirizzare la scelta e l'utilizzo di soluzioni informatiche innovative. Cfr http://www.digitpa.gov.it/altre-attivit%C3%A0/tecnologie-innovative.

580 Vedi www.cnipa.gov.it/site/_files/cnipa_biometria_Alessandroni_041124.ppt.

581 G.U. 13 luglio 2007, n. 161, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1417809.

assicurare elevati e specifici livelli di sicurezza, in relazione a specifiche necessità (…)".

In generale, anche per gli altri interventi dell'Autorità garante sul punto si può osservare che sono stati finalizzati in primo luogo ad assicurare proprio il rispetto dei principi di necessità e proporzionalità nell'utilizzo dei dati biometrici[582]

In ambito comunitario si segnala, inoltre, la creazione di un nuovo progetto finalizzato all'analisi dei quesiti relativi alla tutela dei diritti e sulle opportunità delle tecnologie biometriche, il BITE (*Biometric Identification Technology Ethics*)[583], coordinato dal Prof. Emilio Mordini, direttore del CSSC, il Centro per la Scienza, la Società e la Cittadinanza[584].

6. Privacy e Sicurezza: la questione dei body scanners ed il caso PNR (*Passenger Name Record*)

La crescente domanda di sicurezza che connota la civiltà moderna è percepita soprattutto come richiesta di stabile tutela contro la criminalità e il terrorismo. Viene, invece, spesso tralasciato un altro aspetto, insito al concetto di sicurezza ed altrettanto importante, ovvero quello della sicurezza dei diritti, intesa cioè come istanza di promozione e realizzazione dei diritti al lavoro, ad un ambiente salubre, alla salute, alla giustizia, ecc.

Così, spesso "si evoca l'emergenza per giustificare restrizioni di diritti fondamentali che non assumono i caratteri della provvisorietà, che non sono adottate per fronteggiare il caso, l'evento non previsto dal sistema ordinario, ma si propongono come regole rivolte a durevolmente garantire la sicurezza, il mantenimento dell'ordine sociale" [585].

Per quanto riguarda il diritto alla privacy, in particolare, è stata prospettata un' ingannevole equazione: meno privacy, più sicurezza. Inoltre,

[582] Per gli interventi dell'Autorità garante nel corso del 2009, si veda la Relazione 2009, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1730032.

[583] http://www.biteproject.org/default.asp.

[584] http://www.cssc.eu/index.php.

[585] M. RUOTOLO, *La sicurezza nel gioco del bilanciamento*, Testo della relazione presentata al Convegno "I diversi volti della sicurezza", svoltosi presso l'Università degli Studi di Milano – Bicocca il 4 giugno 2009, consultabile su http://www.associazionedeicostituzionalisti.it/dottrina/libertadiritti/ruotolo_la%20sicurezza%20nel%20gioco%20del%20bilanciamento.pdf.

il riferimento alla privacy ha indotto spesso a pensare che si tratti tutto sommato di modesti sacrifici. In realtà, dietro quella parola si rinvengono "libertà essenziali del nostro tempo e queste non possono essere mai completamente azzerate nella loro sostanza"[586].

Le democrazie, infatti, non possono conoscere sospensioni delle garanzie costituzionali. Il bilanciamento tra valori può variare storicamente, ma esige sempre garanzie adeguate.

Nella società moderna[587], poi, il tema della sicurezza assume una fisionomia che, esasperata sia dall'esigenza di rispondere all'emergenza del terrorismo internazionale dopo gli attentati dell'11 settembre 2001 sia "per effetto dell'invasività delle nuove tecnologie (…)", "investe settori svariati, come ad esempio quello della medicina, dell'economia, dell'ambiente, della protezione della sfera privata. (…)"[588].

Il problema principale è, quindi, quello di trovare le risposte adeguate al crescente bisogno di sicurezza globale. Queste risposte però dovrebbero avere le proprie "direttrici di orientamento nel quadro costituzionale"[589], altrimenti si rischia di cadere nel cd. "paradosso della sicurezza", determinato dall'irraggiungibile obiettivo di cancellare le situazioni di rischio, il cui perseguimento porterebbe a "trasformare lo Stato in un

[586] Cfr S. RODOTà, *L'ansia di sicurezza che cancella i diritti*, consultabile su http://www.privacy.it/rodo20011023.html; S. RODOTà, *Quel conflitto tra pivacy e sicurezza*, consultabile su http://www.privacy.it/rodo20020610.html; R. BIN, *Diritti e argomenti. Il bilanciamento degli interessi nella giurisprudenza costituzionale*, Giuffè, Milano, 1992, 81.

[587] "Il passaggio allo stato pluriclasse, l'ampliamento del catalogo dei diritti, l'assunzione dell'impegno da parte dei pubblici poteri a rimuovere le diseguaglianze al fine di rendere effettivo il godimento dei diritti non potevano non riflettersi sul paradigma del rapporto fra libertà e sicurezza. All'accrescimento degli spazi e del raggio di azione del principio di libertà nello stato costituzionale contemporaneo corrisponde un accrescimento del bisogno di sicurezza, che pure resta sullo sfondo, quasi mai positivizzato nelle costituzioni nazionali, trovando invece risalto nelle carte internazionali e regionali dei diritti e nell'ordinamento europeo", così M. RUOTOLO, *La sicurezza nel gioco del bilanciamento*, op. cit. pag 46; Cfr anche A. D'ALOIA, citato dallo stesso M. RUOTOLO , *Introduzione. I diritti come immagini in movimento: tra norma e cultura costituzionale*, in A. D'ALOIA (a cura di), Diritti e Costituzione, Profili evolutivi e dimensioni inedite,Giuffrè, Milano, 2003, il quale rileva che la sicurezza delle persone e della collettività, pur non trovando spesso menzione nei cataloghi costituzionali dei diritti, "ha mantenuto una qualificazione fondamentale implicita, come situazione retrostante e presupposta rispetto a quella degli altri diritti, spesso identificabili alla stregua di sue declinazioni particolari o strumentali".

[588] P. RIDOLA, *Libertà e diritti nello sviluppo storico del costituzionalismo*, in P. RIDOLA, R. NANIA (a cura di), I diritti costituzionali, II ed., Giappichelli,Torino, 2006, vol. I, pag 143; cfr anche C. SARTORETTI, *Contributo allo studio del diritto alla privacy nell'ordinamento costituzionale*. Riflessioni sul modello francese, op. cit., pag. 91 e ss.

[589] P. RIDOLA, *Libertà e diritti nello sviluppo storico del costituzionalismo*, in P. RIDOLA – R. NANIA (a cura di), I diritti costituzionali, op cit., loc. cit.

soggetto che sa e può tutto e dunque in un fattore di soffocamento della libertà"[590].

Pertanto, la necessità di prevenire tali situazioni di rischio, vista anche negli indicati termini dinamici di "garanzia della continuità nel tempo del godimento di diritti e di aspettative future, attraverso la prevenzione dei bisogni dell'esistenza"[591], non può comportare la regressione e la perdita del valore prioritario di guida individuato nel principio di libertà[592].

Quest'ultimo, infatti, deve "conservare la propria capacità di orientamento nei confronti delle misure adottate in situazioni di emergenza", imponendo, tra l'altro, sia "un'interpretazione rigorosa dei canoni della necessità e della proporzionalità, finalizzata a lasciare off-limits molte misure estreme" sia "la temporaneità delle misure straordinarie"[593].

Pertanto, nell'operare il bilanciamento, "il risalto che le costituzioni del pluralismo conferiscono al principio libertà indirizza giocoforza verso ponderazioni orientate dal canone che configura la libertà come la regola e la sicurezza come l'eccezione"[594].

Queste considerazioni generali valgono anche quando nel gioco del bilanciamento con la sicurezza entra la tutela dei dati personali ed in generale il diritto alla privacy, per il quale si è visto come necessità, proporzionalità e finalità delle misure che in qualche modo lo limitano costituiscono i principi cardini su cui è costruita la relativa disciplina.

6.1. I body scanners

L'utilizzo dei body scanners – usati soprattutto negli aeroporti per controllare che i passeggeri non trasportino oggetti pericolosi o potenziali ordigni – ha visto da sempre contrapporsi il tema della sicurezza con quello della privacy.

[590] P. RIDOLA, op. ult. cit. pag 144; S. NIGER, Le nuove dimensioni della privacy, op. cit., pag 72 e ss.

[591] P. RIDOLA, *Libertà e diritti nello sviluppo storico del costituzionalismo,* op. cit., pag. 144.

[592] M. RUOTOLO, *La sicurezza nel gioco del bilanciamento*, op cit., pag 47; P. RIDOLA, *Libertà e diritti nello sviluppo storico del costituzionalismo*, op. cit.. pag 145.

[593] P. RIDOLA, *Libertà e diritti nello sviluppo storico del costituzionalismo*, op. cit., pag 145.

[594] P. RIDOLA, *Libertà e diritti nello sviluppo storico del costituzionalismo*, op. cit., 146; Cfr. anche M. RUOTOLO, *La sicurezza nel gioco del bilanciamento*, op cit., pag 49.

Esistono principalmente due tipologie di body scanner: una basata sulla riflessione di onde radio ad altissima frequenza (*millimeter wave imaging technology)* e l'altra sulla riflessione all'indietro di raggi X di energia molto bassa (*backscattering*)[595].

I controlli con questo sistema sono stati introdotti negli Stati Uniti dopo gli attentati dell'11 settembre 2001 dall'Agenzia *Trasportation security administration*[596] e si sono via via diffusi nel resto del mondo, Europa ed Italia comprese.

In Italia, il Presidente del Garante per la protezione dei dati personali, Francesco Pizzetti, si è espresso in modo molto prudente in merito al loro impiego nei maggiori aeroporti italiani, evidenziando come anche nel loro uso per la lotta contro il terrorismo, debba essere garantita la dignità della persona, ritenendo opportuno che l'Europa individui in merito un linea comune[597].

Lo stesso, inoltre, ha messo in evidenza come "sia meglio usare delle tecnologie che non consentono la visione immediata e diretta dell'interno del corpo umano ma che ne individuino la sagoma e lancino segnali (acustici o luminosi) in caso di rilevato allarme".

In ogni caso, è importante che la visione del corpo tramite body scanner avvenga "da remoto", non come accade adesso per i bagagli, il cui contenuto passato ai raggi X è visibile da tutti i passeggeri in fila per imbarcarsi[598]

Sul punto, la *Transportation Security Administration* (Tsa) ha affermato che i "body scanners non conservano, stampano, trasmettono né salvano le immagini acquisite. Tutte le macchine sono sprovviste di memoria e le scansioni sono cancellate automaticamente dal sistema non appena gli addetti alla sicurezza hanno provveduto alla loro analisi"[599].

---

[595] Cfr http://tg24.sky.it/tg24/cronaca/2010/01/05/body_scanner_ecco_come_funziona.html; http://www.mondohightech.com/software-e-nuove-tecnologie/che-tipi-di-body-scanner-esistono-e-come-funzionano/; http://epic.org/privacy/airtravel/backscatter/.

[596] www.tsa.gov.

[597] S. ROSSI, *Body Scanner*, articolo pubblicato il 31 dicembre 2009 su http://it.reuters.com/article/topNews/idITMIE5BU0BT20091231.

[598] "E' evidente che se adottassimo un body scanner con il visore visibile da altri soggetti sarebbe una cosa assolutamente inaccettabile. Il controllo deve avvenire 'da remoto', cioè lo scanner è lì (davanti a tutti) ma il soggetto che visiona il passaggio è 'da remoto' (ovvero lontano)" cfr S. ROSSI, *Body Scanner*, art. cit.

[599] M. QUATRARO, *Body scanner negli aeroporti in Italia:paura per la salute. Privacy a rischio con immagine spedite*?, articolo consultabile su http://www.businessonline.it/news/9719/Body-scanner-negli-aeroporti-in-Italia-paura-per-la-salute-privacy-a-rischio-con-immagine-spedite.html.

A contraddire questa affermazione sono però i membri dell'*Electronic Privacy Information Center* (Epic)[600] che, al contrario di quanto affermato dalla Tsa, ritengono che i dispositivi in questione non solo sono in grado di conservare le immagini, catturate durante l'analisi dei passeggeri sottoposti a scansione, ma sono anche dotati di funzionalità per l'invio delle stesse.

La Tsa ha sempre negato l'esistenza di simili strumenti, tuttavia dalle specifiche di costruzione, contenute in un documento sottoscritto proprio dall'autorità dei trasporti Usa, sembrerebbe emergere che tutti i body scanners debbano essere in grado, invece, di archiviare e inoltrare le immagini[601].

Sulla questione ha preso posizione anche il Commissario europeo per la Giustizia e i diritti umani, Viviane Reding, dichiarando che non è attraverso questo dispositivo che si potranno risolvere tutte le problematiche legate alla sicurezza dei voli e degli aeroporti[602].

La Reding, poi, ha aggiunto di essere contraria all'obbligatorietà dei controlli attraverso la scansione corporale per ogni passeggero in partenza dagli aeroporti dell'UE. "I cittadini non sono oggetti" perciò è necessario proteggere la loro privacy e la loro dignità, ricercando sistemi meno invasisi per l'individuazione di esplosivi. Questo perché, secondo la Reding, "l'esigenza della sicurezza non può giustificare qualsiasi violazione della privacy dei cittadini".

Il Commissario europeo ha così individuato tre condizioni essenziali per l'introduzione dei macchinari negli aeroporti europei: la volontarietà, l'immediata distruzione delle immagini, successiva all'esito negativo del controllo e la disposizione di imminenti verifiche sulle conseguenze per la salute. "Abbiamo bisogno di una linea chiara – precisa il Commissario dell'UE – che non sia mossa dalla paura e che si basi sulla difesa dei valori fondanti dell'Unione, anche quando negoziamo a livello internazionale".

---

600 http://epic.org/- Il 2 luglio 2010 l'Epic ha presentato una petizione di modifica urgente, chiedendo al Corte d'Appello del Distretto della Columbia la sospensione del programma "full-body scanner" della Transportation Security Administration(TSA), in quanto "unlawful, invasive, and ineffective." Cfr http://epic.org/privacy/airtravel/backscatter/.

601 M. QUATRARO, *Body scanner negli aeroporti in Italia:paura per la salute. Privacy a rischio con immagine spedite?*, art. cit.; cfr il rapporto dell'Electronic Privacy Information Center su http://epic.org/.

602 E. BALLACCI, *UE, Reding: "Contraria ai body scanner, urgono verifiche"*, articolo consultabile su http://www.newnotizie.it/2010/01/13/ue-reding-contraria-ai-body-scanner-urgono-verifiche/.

Identica è anche la posizione del Gruppo di lavoro "art. 29", il quale, in un precedente parere del febbraio 2009[603], dopo aver chiarito che il body scanner ha come obiettivo l'individuazione di oggetti e non quello di catturare immagini del corpo, ha affermato che occorrerebbe valutarne la compatibilità con la Carta dei diritti fondamentali dell'Unione europea, la CEDU e la Direttiva 95/46/CE[604]. Il Gruppo di lavoro ha concluso che al momento attuale non ci sono prove che dimostrino la necessità di utilizzare un tale strumento.

Il 15 giugno 2010 la Commissione europea ha pubblicato una Comunicazione al Parlamento ed al Consiglio avente ad oggetto l'uso dei body scanners negli aeroporti europei[605] , in cui è stato evidenziato che i differenti standard di scanner utilizzati in Europa comportano il serio rischio di frammentare i diritti fondamentali dei cittadini dell'Unione europea, impedendo la loro libertà di movimento ed aumentando le preoccupazioni per la salute in relazione alle nuove tecnologie della sicurezza.

Quindi, mentre l'utilizzo degli scanners è ancora un'eccezione negli aeroporti europei, cresce la necessità di affrontare in breve tempo questi argomenti e trovare una soluzione comune"[606].

"Test formali per l'introduzione dei body scanners come metodo primario di controllo dei passeggeri sono stati introdotti in Finlandia - aeroporto Vantaa di Helsinki - in Gran Bretagna, all'aeroporto londinese di Heatrow e si stanno predisponendo nell'aeroporto di Manchester, e in Olanda, nell'aeroporto Shiphol di Amsterdam. Anche la Francia e l'Italia

[603] Consultabile su http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2009_05_11_annex_consultation _letter_chairman_art29wp_daniel_calleja_dgtren_en.pdf.

[604] Cfr pag 12 del Parere, nel quale, tra l'altro si legge:"There is a close link between privacy, protection of personal data, human dignity and *phisical integrity* in relation to use of body scanner. Altought the answer below focus on privacy and data protection, the evaluation of body scanners on the privacy of individuals should necessarily take into account the intrusion in relation to their human dignity and physical integrity (…). The introduction of body scanners would depend on their clearly established *necessity*, on the balance between their necessity and the fundamental rights of the individuals, and on the nature of rule and safeguards put in place".

[605] COM(2010) 311 final, 15.6.2010, consultabile in inglese su http://ec.europa.eu/transport/air/security/doc/com2010_311_security_scanners_en.pdf. .

[606] "Different standards of scanners currently deployed in Europe bring a serious risk of fragmenting fundamental rights of EU citizens, impeding their rights of free movement and escalating their health concerns related to new security technologies. While Security Scanners are still exceptional at European airports, there is a growing need to swiftly address these concerns and find a common solution", COM(2010) 311 final, 15.6.2010, cit..

hanno iniziato i test. Allo stato la Commissione non è a conoscenza di test in altri Stati membri"[607].

Il punto di partenza del ragionamento della Commissione è stato che "tutta la legislazione dell'Unione europea, compresa quella sulla sicurezza aerea e la relativa applicazione, deve rispettare completamente i diritti fondamentali e gli standard di sicurezza per la salute, stabiliti e protetti dalla normativa europea"[608].

"I diritti fondamentali sono protetti dalla Carta dei diritti fondamentali dell'Unione europea e dalla diversa legislazione comunitaria di secondo grado. Per quanto riguarda i body scanners ai fini di sicurezza, devono essere menzionati, in particolare, la dignità umana (art. 1), il rispetto della vita privata e familiare (art 7), la libertà di pensiero, di coscienza, di religione (art. 10), il diritto a non essere discriminati (art.21), il diritto dei minori (art. 24) e la garanzia di un elevato livello di protezione della salute umana nella definizione e nello sviluppo in tutte le politiche e le attività dell'Unione (art. 35)"[609].

Il rispetto dei diritti garantiti dalla Carta e dalla legislazione comunitaria, secondo la Commissione, implica in linea di principio la non adozione di misure che riducano tali diritti. In ogni caso, l'introduzione di qualsiasi limitazione deve avvenire per legge e rispettare, comunque, l'essenza di quei diritti.

Inoltre, ogni limitazione deve essere giustificata, il che significa che deve essere necessaria ed in grado di raggiungere gli obiettivi di pubblico interesse - tra cui la sicurezza aerea - riconosciuti dall'Unione europea e deve, poi, rispettare il principio di proporzionalità.

---

607 "Formal trials of Security Scanners as a primary method for screening passengers were undertaken in Finland, at Helsinki -Vantaa airport, in the UK, at London Heathrow airport and are ongoing at Manchester airport2, and in the Netherlands, at Amsterdam Schiphol airport. Recently also France and Italy have begun testing. To Commission's knowledge no other Member States deploy Security Scanners", COM(2010) 311 final, 15.6.2010, cit..

608 "All'EU legislation, including legislation on aviation security, and its application must fully comply with fundamental rights and health standards established and protected by European Union law", COM(2010) 311 final, 15.6.2010, cit..

609 Fundamental rights are protected by the Charter of Fundamental Rights of the European Union and by several acts of secondary EU legislation. In the context of Security Scanners in particular human dignity (Article 1), respect for private and family life (Article 7), protection of personal data (Article 8), freedom of thought, conscience and religion (Article 10), non-discrimination (Article 21), the rights of the child (Article 24) and ensuring a high level of human health protection in the definition and implementation of all Union's policies and activities (Article 35) must be mentioned.", COM(2010) 311 final, 15.6.2010, cit..

Dalle suddette importanti ed imprescindibili premesse, la relazione ha continuato analizzando le diverse tecnologie utilizzate per i body scanners ed i loro impatti, in termini di efficienza, sia per i controlli di sicurezza sia per la tutela del soggetto interessato.

La Commissione ritiene che sia possibile trovare il giusto equilibrio fra i differenti interessi e che, quindi, questa tecnologia, se adeguatamente disegnata ed utilizzata, può essere una possibile via da seguire, per realizzare l'obiettivo di rafforzare le norme in materia di sicurezza aerea in Europa, agevolando allo stesso tempo i viaggiatori.

Tuttavia, per la Commissione è altresì evidente che i body scanners da soli, così come qualsiasi altra misura, non possono garantire la sicurezza aerea al 100%. Questa può scaturire solo da una combinazione di interventi, supportati da una forte cooperazione internazionale e da un alto livello di "intelligence".

E' necessario, quindi, un approccio comune, l'unico davvero in grado di garantire un'applicazione uniforme delle regole e degli standard per la sicurezza in tutti gli aeroporti dell'Unione europea. Questo è fondamentale per tutelare sia la sicurezza aerea sia i diritti fondamentali dei cittadini e la loro salute.

Inoltre, proprio in relazione alla salute, lo sviluppo della tecnologia degli scanner richiede un rigoroso e accurato studio scientifico sui rischi che questo tipo di tecnologia può avere. Infatti, gli studi attuali, sugli effetti associati all'esposizione a radiazioni ionizzanti, giustificano una particolare prudenza nell'adozione di queste radiazioni negli scanner per la sicurezza[610].

Per quanto riguarda l'eventuale obbligatorietà delle misure, la Commissione ha osservato che deve essere tenuto in considerazione che, secondo le regole vigenti per (es. la ricerca manuale o il passaggio attraverso il metal detector), non è offerta scelta al passeggero di rifiutare i controlli in questo momento utilizzati.

[610] "Only a EU approach would legally guarantee uniform application of security rules and standards throughout all EU airports. This is essential to ensure both the highest level of aviation security as well as the best possible protection of EU citizens' fundamental rights and health. The deployment of any security scanner technology requires a rigorous scientific assessment of the potential health risks that such technology may pose for the population. Scientific evidence documents the health risks associated with exposure to ionising radiation. It justifies particular precaution in considering the use of such radiation in Security Scanners", COM(2010) 311 final, 15.6.2010, cit..

Al fine di evitare un livello di sicurezza a "macchia di leopardo", quindi, secondo la Commissione gli individui dovrebbero poter modificare questi processi solo per la tutela di diritti fondamentali o per ragioni di salute, dove esistano metodi alternativi che offrano equivalenti garanzie di sicurezza[611].

Tuttavia, i presupposti prima individuati dalla stessa Commissione nella relazione, quali il principio di necessità e proporzionalità, in realtà, dovrebbero portare a ritenere che se esistono metodi meno invasi, ma altrettanto efficaci ai fini della sicurezza, quest'ultimi dovrebbero essere senz'altro preferiti o quantomeno dovrebbe esser data al passeggero la possibilità di scegliere a quale controllo sottoporsi.

Per quanto riguarda, poi, la tutela dei dati personali, la relazione ha evidenziato che l'acquisizione attraverso gli scanners ed il trattamento delle immagini di un individuo, al fine di consentire ad una persona addetta al controllo di verificarne la sicurezza, ricadono nell'ambito di applicazione della legislazione europea a tutela dei dati personali.

Questo comporta che il soggetto, la cui immagine deve essere presa tramite i "*Security Scanners*", è previamente informato di essere soggetto a tale controllo e della finalità dello stesso.

In merito, la Commissione ha insistito molto sulla necessità di assicurare al pubblico un'informazione adeguata, comprensibile e chiara su tutti gli aspetti legati all'uso degli scanners per la sicurezza aerea[612].

Le immagini, inoltre, devono essere raccolte e trattate nel rispetto dei principi stabiliti per la tutela dei dati personali e utilizzate solo per la finalità di garantire la sicurezza aerea.

In linea di principio, quindi, le immagini non dovrebbero essere memorizzate e successivamente recuperate, una volta risultato evidente che il soggetto non trasposta oggetti o materiali pericolosi. Solo nel caso in cui

611 "As regards the question whether or not Security Scanners should be compulsory it has to be taken into account that under the existing rules and regarding the screening methods recognised today (hand search, walk through metal detector, etc.), passengers are not offered any possibility to refuse the screening method or procedure chosen by the airport and/or the screener in charge. In order not to jeopardize high levels of aviation security, unpredictability of security processes at airports is an important consideration. This being so, individuals should only be able to influence these processes for fundamental rights or health reasons where alternative methods would offer equivalent security guarantees.", COM(2010) 311 final, 15.6.2010, cit..

612 "Moreover, appropriate, comprehensive and clear information to the public on all aspects of Security Scanners use in aviation security should be also ensured" , COM(2010) 311 final, 15.6.2010, cit..

la persona venisse fermata, perché possiede oggetti proibiti, l'immagine potrebbe essere memorizzata fino a che il passeggero non sia definitivamente messo in sicurezza o non gli sia, invece, negato l'accesso alle aree riservate ed eventualmente all'aereo.

La Commissione, infine, ha sottolineato l'utilità delle tecnologie *privacy by design* e delle *privacy enhancing technologies*, già segnalate in questa sede in riferimento ad internet. Queste, infatti, applicate ai software ed agli hardware degli scanner potrebbero contribuire a salvaguardare il corretto trattamento dei dati raccolti.

Un'altra soluzione in tal senso è stata individuata nel cd. *Automatic Threat Recognition* (ATR). Questi sistemi possono essere utilizzati sia per assistere l'addetto al controllo, nell'interpretazione delle immagini, sia per ottenere quest'ultima automaticamente.

Proprio tale possibilità è stata vista favorevolmente dalla Commissione, in quanto lo sviluppo di questa tecnologia potrebbe portare in futuro a non richiedere più la presenza umana nello svolgimento dei controlli tramite body scanner. Al responsabile della sicurezza sarebbe così visibile solamente il risultato del processo automatico di ricerca (allarme e localizzazione dell'oggetto sulla persona/nessun allarme).

6.2. Il caso PNR (*Passenger Name Racord*)

I dati PNR (*Passenger Name Record*) sono informazioni non verificate fornite dai passeggeri e raccolte dai vettori aerei, ai fini della prenotazione e delle operazioni di check-in, e riguardano il viaggio di ciascun passeggero, sono conservati nei sistemi di prenotazione e di controllo delle partenze dei vettori aerei.

Questi dati contengono vari tipi di informazioni, come la data del viaggio, l'itinerario, elementi sull'emissione del biglietto, i recapiti (quali l'indirizzo e i numeri di telefono), l'agente di viaggio, le modalità di pagamento, il numero di posto assegnato e le informazioni relative al bagaglio.

I metodi di trasmissione utilizzati per i dati sono chiamati "*push*" e "*pull*". La differenza principale è che nel metodo "*push*" i dati sono trasmessi dal vettore aereo all'autorità nazionale, mentre nel metodo "*pull*" è l'autorità

nazionale che ottiene l'accesso al sistema di prenotazione del vettore aereo ed estrae i dati.

Deve essere precisato, però, che i dati PNR sono diversi dai dati API (*Advance Passenger Information*); questi ultimi sono dati anagrafici raccolti dalla banda a lettura ottica del passaporto e comprendono il nome, il luogo di residenza, il luogo di nascita e la cittadinanza dell'interessato. Ai sensi della Direttiva API[613], tali dati sono messi a disposizione delle autorità di controllo alla frontiera solo per i voli diretti verso l'UE al fine di migliorare i controlli alle frontiere e combattere l'immigrazione illegale.

Sebbene la direttiva permetta di utilizzare i dati API per altre finalità di applicazione normativa, tale uso costituisce l'eccezione e non la regola. I dati API sono conservati dagli Stati membri per 24 ore.

Oltre ai dati API, alcuni paesi impongono ai vettori aerei di trasmettere anche i suddetti dati PNR[614]. Questi sono usati per combattere il terrorismo e altri reati gravi, quali la tratta di esseri umani e il traffico di stupefacenti.

In realtà i dati PNR sono usati da quasi 60 anni, perlopiù dalle autorità doganali ma anche dalle autorità di contrasto in tutto il mondo. Ciò nondimeno, fino a poco tempo fa non era tecnologicamente possibile accedere in anticipo e elettronicamente a tali dati, pertanto, se ne limitava l'uso al trattamento manuale e solo per alcuni voli. Le tecnologie odierne permettono, ormai, la trasmissione elettronica anticipata di questi dati.

Tuttavia, poiché le norme di protezione dei dati vigenti nell'UE vietano ai vettori aerei, che effettuano voli in partenza dall'UE, di trasmettere i dati PNR dei loro passeggeri a Paesi terzi che non garantiscono un adeguato livello di protezione dei dati personali, senza che siano addotte garanzie appropriate, quando gli Stati Uniti, il Canada e l'Australia hanno richiesto ai vettori aerei di trasmettere i dati PNR per i voli diretti in quei paesi, i vettori si sono trovati in una situazione alquanto delicata.

[613] Direttiva n. 2004/82/CE del Consiglio, del 29 aprile 2004, concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate.

[614] Alcuni paesi (Stati Uniti, Canada, Australia, Nuova Zelanda e Corea del Sud) usano già i dati PNR a fini di contrasto. Altri (Giappone, Arabia Saudita, Sudafrica e Singapore) hanno emanato leggi in materia e/o stanno testando l'uso dei dati PNR. Molti altri paesi extra comunitari hanno iniziato a valutare l'opportunità di usare i dati PNR ma non hanno ancora emanato leggi al riguardo. All'interno dell'Unione, il Regno Unito ha già introdotto un sistema PNR. La Francia, la Danimarca, il Belgio, la Svezia e i Paesi Bassi dispongono della pertinente legislazione e/o stanno testando l'uso dei dati PNR. Molti altri Stati membri stanno valutando l'opportunità di istituire sistemi PNR.

L'UE è dovuta intervenuta, quindi, e ha negoziato accordi internazionali distinti con questi tre Paesi[615], rendendo possibile il trasferimento dei dati PNR al di fuori dell'UE, alle autorità di tali Paesi.

La vicenda che ne è scaturita, soprattutto in relazione agli accordi con gli Stati Uniti, è particolarmente rilevante perché da un lato esemplificativa di come, in concreto, vengano in rapporto la tutela dei diritti fondamentali e le esigenze di sicurezza e, dall'altro, perché mette chiaramente in evidenza come la suddetta questione si ponga in termini sovranazionali.

Caratteristica quest'ultima che si è indicata più volte esser tipica dello sviluppo sociale, politico e giuridico, oltre che tecnologico, contemporaneo.

Come già evidenziato, a seguito degli attentati terroristici dell'11 settembre sono stati approvati numerosi atti legislativi volti a combattere il terrorismo ed a tutelare la sicurezza nazionale.

Così, negli Stati Uniti, sulla sicurezza aerea, sono state stabilite diverse disposizioni[616], secondo le quali ogni compagnia aerea, in volo per (o da) gli Stati Uniti, deve consentire al *Bureau of Customs and Border Protection*[617] l'accesso elettronico ai dati PNR, contenuti nel sistema automatico di prenotazione e partenze dei voli aerei.

Nel giungo 2002, tuttavia, la Commissione europea ha informato le autorità americane che, sebbene condivisibili, le misure di sicurezza predisposte avrebbero potuto entrare in conflitto con alcune disposizioni comunitarie a tutela dei dati personali, in particolare la Direttiva n. 95/46/CE ed il regolamento sull'uso dei sistemi computerizzati di prenotazione[618].

Pertanto, al termine delle trattative avviate di conseguenza, il 1 marzo 2004 la Commissione ha presentato al Parlamento europeo un bozza di

---

615 Accordo PNR CE-USA del 2004 (GU L 183 del 20.5.2004, pag. 84) e decisione della Commissione del 14 maggio 2004 (GU 235 del 6.7.2004, pag. 11); Accordo PNR UE-USA del 2006 (GU L 298 del 27.10.2006, pag. 29) e lettere di accompagnamento (GU C 259 del 27.10.2006, pag. 1), accordo PNR UE-USA del 2007 (GU L 204 del 4.8.2007, pag. 18), accordo PNR UE-Canada (GU L 82 del 21.3.2006, pag. 15 e GU L 91 del 29.3.2006, pag. 49) e accordo PNR UE-Australia (GU L 213 dell'8.8.2008, pag. 47).

616 l'Aviation and Transportation Security Act del 19 novembre 2001 ed i regolamenti Passenger and Crew Manifest in Foreign Air Transportation to United States e Passaneger Name Record Information Required for Passengers in Flights in Foreign Air Transportation to or from the United States. Cfr U. PAGALLO, *La tutela della privacy negli Stati Uniti d'America e in Europa*, op. cit. pag. 159.

617 www.cbp.gov.

618 Regolamento relativo a un codice di comportamento in materia di sistemi telematici di prenotazione e che abroga il regolamento (CEE) n, 2299/89, n 80/1009, del 4 febbraio 2009, GUUE L35/47, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:035::0047:0055:IT:PDF.

decisione sul giudizio di adeguatezza, ex art 25 della Direttiva n. 95/46/CEE, e poco dopo ha depositato in Parlamento la bozza dell'accordo che, in nome della Comunità, il Consiglio avrebbe dovuto firmare con gli Stati Uniti.

Nella Risoluzione del 31 marzo 2004, però, il Parlamento ha eccepito che la Commissione con la suddetta iniziativa era andata oltre le proprie competenze, ritenendo che, nel caso specifico, sarebbe stato più appropriato un accordo internazionale nel rispetto dei diritti fondamentali.

Successivamente, non vedendo accolto l'invito né dal Consiglio né dalla Commissione, il Parlamento ha chiesto formalmente alla Corte di Giustizia di esprimere un'opinione sulla compatibilità degli accordi proposti dalla Commissione e dal Consiglio con le disposizioni del Trattato.

Nonostante ciò, il 14 maggio 2004, la Commissione ha adottato la decisione positiva sul livello adeguato di protezione dei dati PNR trasferiti dalla compagnie aeree alle autorità americane ed il 17 maggio, a sua volta, il Consiglio ha approvato l'accordo tra la Comunità europea e gli Stati Uniti.

Preso atto delle suddette iniziative, il 9 luglio 2004 il Parlamento ha ritirato la richiesta di opinione, impugnando sia la decisione n. 2004/496/CE del Consiglio sia la decisione della Commissione n. 2004/535/Ce, rispettivamente nelle cause C-317/04 e C-318/04[619].

La Corte di Giustizia con la decisione del 30 maggio 2006 ha annullato i suddetti atti, in quanto, secondo la Corte, adottati al di fuori delle rispettive sfere di competenza della Commissione e del Consiglio, ritenendo poi inutile esaminare oggetto e principi contesi nella lite.

Nuove trattative sono state perciò iniziate, questa volta condotte non dalla Commissione o dal Consiglio bensì dall'Unione europea, e ad ottobre del 2006 è stato adottato – a firma del Presidente dell'Unione europea – un nuovo accordo, con la previsione però di un termine per il nuovo regime, stabilito al 31 luglio 2007.

Un successivo accordo è stato, di conseguenza, firmato il 23/26 luglio 2007, con riserva di conclusione in una data successiva[620]. Conformemente

[619]Per un'analisi approfondita delle motivazioni delle parti in causa, si rinvia a U. PAGALLO, *La tutela della privacy negli Stati Uniti d'America e in Europa*, op. cit., pag. 164 e ss.; la sentenza è consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62004J0317:IT:PDF.

[620] Cfr. la Decisione n. 5274/10 del Consiglio relativa alla conclusione dell'accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e sul trasferimento dei dati del codice di prenotazione (Passenger Name Record, PNR) da parte dei vettori aerei al Dipartimento per la sicurezza interna degli

al punto 9 dell'accordo, questo è applicato in via provvisoria dalla data della sua firma.

La nuova intesa ha previsto rilevanti modifiche rispetto agli accordi del 2004 e 2006, tra cui la riduzione dei dati trattati – da trentaquattro a diciannove – ed il diritto di accesso ai dati indipendentemente dalla cittadinanza o dal luogo di residenza.

Non di meno anche in questo caso non sono mancati dubbi e perplessità. L'obiezione più forte del Parlamento europeo ha riguardato, ad esempio, il fatto che l'accordo concedeva alle autorità statunitensi il diritto di trasferire anche a Paesi terzi i dati PNR dei passeggeri, ottenuti dalle compagnie aeree europee, a condizioni fissate unilateralmente dagli Stati Uniti.

In particolare, il Parlamento ha ritenuto molto grave che l'Unione europea si fosse impegnata espressamente a non interferire sul trasferimento di dati PNR di cittadini europei a Paesi terzi, rinunciando ad esercitare il proprio diritto e dovere di protezione in questa materia[621].

Il Parlamento ha manifestato, inoltre, preoccupazione per il fatto che il trattamento, la raccolta, l'utilizzo e la conservazione dei dati PNR da parte del Dipartimento per la sicurezza interna degli USA non fosse fondata "su un accordo vero e proprio, ma soltanto su assicurazioni non vincolanti che possono essere cambiate unilateralmente dal dipartimento in qualsiasi momento e che non conferiscono alcun diritto o beneficio ad alcuna persona o parte"[622].

Lo stesso Parlamento ha evidenziato, poi, "la definizione non chiara degli obiettivi nella lettera del dipartimento, in cui si nota che i dati del PNR possono essere utilizzati ai fini della lotta contro il terrorismo e reati connessi, ma anche per una serie di scopi addizionali non specificati, segnatamente 'per la protezione degli interessi vitali della persona interessata o di altre persone, o in qualsiasi procedimento giudiziario di natura penale o in qualsiasi altro modo conforme alla legge'"[623].

Stati Uniti (DHS) (Accordo PNR del 2007), consultabile su http://www.parlamento.it/web/docuorc2004.nsf/00672360b4d2dc27c12576900058cad9/1fb60c5ecea1255bc12576ab006601c8/$FILE/05274-10_IT.PDF

621 Risoluzione del Parlamento europeo del 12 luglio 2007 sull'accordo PNR con gli Stati Uniti d'America, consultabile su http://www.delegazionepse.it/canali.asp?id=10376.

622 Punto 6 della Risoluzione del Parlamento europeo, cit.

623 Punto 7 della Risoluzione del Parlamento europeo, cit.

L'Assemblea europea ha così ricordato che "l'accordo amministrativo" concluso tra l'UE e gli USA non deve avere l'effetto di ridurre il livello di protezione dei dati personali, garantito dalle legislazioni nazionali degli Stati membri, deplorando l'ulteriore confusione che esso avrebbe creato per quanto riguarda gli obblighi delle compagnie aeree UE e i diritti fondamentali dei cittadini UE.

Infine, la stessa si è manifestata molto critica e scettica sulla possibilità di adozione di un sistema PNR anche a livello europeo[624]

Con l'entrata in vigore del trattato di Lisbona il 1° dicembre 2009[625], sono cambiate però le norme e le competenze. In particolare, in quest'ambito, l'Unione europea deve seguire le procedure previste dall'articolo 218 del Trattato sul funzionamento dell'Unione europea[626].

Il Parlamento è chiamato ora ad approvare gli accordi dell'Unione europea sul trasferimento dei dati del codice di prenotazione (dati PNR), ai fini della conclusione di tali accordi.

Per questo motivo, il 5 maggio 2010 è stata adottata dallo stesso una Risoluzione, avente ad oggetto l'avvio dei negoziati per la conclusione di accordi sui dati del codice di prenotazione (PNR) con gli Stati Uniti, l'Australia e il Canada[627].

In tale documento, il Parlamento ha ribadito che "nell'attuale era digitale, la protezione dei dati, il diritto all'autodeterminazione informativa, i diritti personali e il diritto alla privacy sono diventati valori che svolgono un ruolo sempre maggiore e devono pertanto essere tutelati con particolare attenzione". Quindi, ha rammentato la propria determinazione a combattere il terrorismo e la criminalità organizzata transnazionale e, allo stesso tempo, la ferma convinzione della necessità di proteggere le libertà

[624] Punti 26-27-28 della Risoluzione del Parlamento europeo, cit.; si veda anche la Proposta di Decisione quadro della Commissione europea del 6.11.2007, consultabile su http://www.garanteprivacy.it/garante/document?ID=1531454. Su quest'ultima si veda il parere comune del Gruppo di lavoro Articolo 29 per la protezione dei dati personali ed il Gruppo di lavoro per la cooperazione giudiziaria e di polizia, 02422/07/IT, consultabile su http://www.garanteprivacy.it/garante/document?ID=1531958. Si ricorda, inoltre, che ai sensi la direttiva 2004/82/CE del Consigli i vettori aerei hanno l'obbligo di trasmissione anticipata dei dati relativi alle persone trasportate (*Advance Passenger Information* (API)) alle competenti autorità nazionali.

[625] http://europa.eu/lisbon_treaty/index_it.htm.

[626] GUUE C 83 30.3.2010, consultabile su http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2010:083:SOM:IT:HTM.

[627] P7_TA-PROV(2010)0144, consultabile su http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2010-0144&language=IT&ring=B7-2010-0244.

civili e i diritti fondamentali, assicurando il massimo rispetto della privacy, dell'autodeterminazione informativa e della protezione dei dati.

In tal senso i principi di necessità e di proporzionalità sono, perciò, fondamentali per condurre con efficacia la lotta al terrorismo.

L'Assemblea ha sottolineato, inoltre, che l'Unione europea è fondata sullo stato di diritto e che qualsiasi trasferimento di dati personali da parte dell'Unione europea e dei suoi Stati membri verso Paesi terzi, a fini di sicurezza, deve basarsi su accordi internazionali aventi il rango di atti legislativi. Questo è necessario al fine di offrire le necessarie garanzie ai cittadini dell'Unione, rispettare le garanzie procedurali e i diritti della difesa nonché ottemperare alla normativa sulla protezione dei dati a livello nazionale ed europeo.

Con tale la Risoluzione il Parlamento ha deciso, pertanto, di rinviare la votazione sulla richiesta di approvazione degli accordi con gli Stati Uniti e l'Australia, fino a quando non avrà esaminato le possibili modalità di utilizzo dei dati PNR che siano conformi al diritto dell'Unione e tengano conto delle preoccupazioni espresse dallo stesso, nelle precedenti risoluzioni sui dati PNR.

In ogni caso, l'Assemblea ha sottolineato che qualsiasi nuovo strumento legislativo deve essere preceduto da una valutazione d'impatto sulla privacy e da un test di proporzionalità che dimostri l'insufficienza degli strumenti giuridici esistenti.

E' indispensabile, poi, che questi accordi prevedano opportuni meccanismi di revisione indipendente e di vigilanza giuridica nonché di controllo democratico.

Il Parlamento ha invitato, inoltre, la Commissione a richiedere quanto prima che l'Agenzia per i diritti fondamentali dell'Unione europea fornisca un parere circostanziato sulla dimensione dei diritti fondamentali di qualsiasi nuovo accordo PNR e che vengono stabiliti un'unica serie di principi, i quali fungano da base per gli accordi con Paesi terzi.

A tal fine lo stesso ha individuato alcuni requisiti minimi che tale modello dovrebbe soddisfare, tra cui il principio di pertinenza, finalità e non eccedenza, nella richiesta e trattamento dei dati, l'utilizzo del metodo

"*push*" per il trasferimento dei dati, il divieto di utilizzo dai dati per la ricostruzione di profili[628].

Alla suddetta risoluzione ha fatto seguito la Comunicazione della Commissione, sull'approccio globale al trasferimento dei dati PNR verso Paesi terzi[629].

La Comunicazione ha come obiettivo principale di istituire, per la prima volta, un insieme di criteri generali su cui basare i futuri negoziati per la conclusione di accordi PNR con i Paesi terzi.

In questo modo le raccomandazioni della Commissione relative ai negoziati per gli accordi PNR con i Paesi terzi in futuro "dovranno quanto meno rispettare i criteri generali stabiliti nella comunicazione, fermo restando che ogni raccomandazione potrà fissare criteri aggiuntivi"[630].

Secondo la Commissione, quindi, "l'approccio globale ai dati PNR dovrebbe enunciare le norme generali che gli accordi internazionali tra l'UE e i paesi terzi dovrebbero rispettare per garantire la maggiore coerenza possibile per quanto riguarda le garanzie di protezione dei dati che tali paesi dovranno applicare e le modalità di trasmissione dei dati da parte dei vettori aerei".

---

[628] "a) i dati PNR possono essere utilizzati soltanto ai fini delle attività di contrasto e della sicurezza in caso di grave criminalità organizzata transnazionale o di terrorismo a livello transfrontaliero, sulla base delle definizioni giuridiche stabilite nella decisione quadro 2002/475/GAI del Consiglio, del 13 giugno 2002, sulla lotta contro il terrorismo e nella decisione quadro del Consiglio 2002/584/GAI, del 13 giugno 2002, relativa al mandato d'arresto europeo;

b) l'impiego dei dati PNR ai fini delle attività di contrasto e della sicurezza deve essere conforme alle norme europee sulla protezione dei dati, in particolare per quanto riguarda la limitazione delle finalità, la proporzionalità, il meccanismo giuridico di ricorso, la limitazione della quantità di dati c) da raccogliere e della durata dei periodi di conservazione;

c) in nessun caso i dati PNR possono essere utilizzati a scopo di estrazione dei dati o di "profiling" (studio dei profili); non può essere adottata nessuna decisione di divieto di volo o di indagare o perseguire un individuo sulla sola base di tali ricerche automatizzate o consultazione di banche di dati; l'uso dei dati deve essere limitato a reati o minacce specifici, caso per caso;

d) in caso di trasferimento di dati PNR di cittadini UE verso paesi terzi, le condizioni di tale trasferimento sono stabilite in un trattato internazionale vincolante, che garantisca certezza del diritto e parità di trattamento ai cittadini e alle imprese dell'Unione;

e) il trasferimento successivo di dati da parte del paese destinatario verso paesi terzi deve essere conforme alle norme UE sulla protezione dei dati, che andranno stabilite mediante un accertamento specifico dell'adeguatezza; ciò deve applicarsi altresì a qualsiasi eventuale trasferimento successivo di dati da parte del paese destinatario verso paesi terzi;

f) i dati PNR possono essere concessi unicamente sulla base del metodo PUSH;

g) i risultati saranno immediatamente condivisi con le autorità competenti dell'UE e degli Stati membri;". P7_TA-PROV(2010)0144, cit.

[629] COM(2010) 492 finale, 21.9.2010, consultabile su http://www.parlamento.it/web/docuorc2004.nsf/8fc228fe50daa42bc12576900058cada/3ef3b565662ec4ecc12577ab0031dbb0/$FILE/COM2010_0492_IT.pdf.

[630] COM(2010) 492 finale, 21.9.2010, cit.

A tal fine sarà fondamentale, inoltre, che l'UE predisponga meccanismi per controllare la corretta attuazione degli accordi - ad esempio le verifiche periodiche congiunte - ed efficaci procedimenti di composizione delle controversie.

In merito alla tutela dei dati personali, la Comunicazione ha precisato che, data la possibilità che i sistemi di protezione dei dati dei Paesi terzi possano differire dalla protezione dei dati garantita nell'UE, è importante che, per i trasferimenti di dati PNR verso Paesi terzi, quest'ultimi garantiscano un livello adeguato di protezione dei dati in forza di una solida base giuridica.

Tale livello adeguato può essere previsto dalla legislazione del Paese terzo o da impegni giuridicamente vincolanti, inseriti nell'accordo internazionale che disciplina il trattamento dei dati personali.

Ad ogni modo, la Commissione ha elencato alcuni principi che i Paesi terzi richiedenti dovrebbero rispettare. Questi principi riguardano, fra gli altri, le finalità di raccolta, l'utilizzo di dati sensibili solo in "circostanze eccezionali", la sicurezza dei dati, la supervisione da parte di "un'autorità pubblica indipendente incaricata della protezione dei dati e dotata di effettivi poteri d'intervento e contrasto", la trasparenza e l'obbligo di informazione, i diritti di accesso, rettifica e cancellazione dei propri dati PNR, il diritto ad un ricorso in sede amministrativa e giudiziaria, il periodo di conservazione dei dati e restrizioni dei successivi trasferimenti ad altre autorità o ad altri Paesi terzi[631].

La Comunicazione è stata accolta favorevolmente dal Parlamento con la Risoluzione dell'11 novembre 2010[632], nella quale, tuttavia, sono state anche ribadite le posizioni, precedentemente espresse sulla materia, e si è invitata nuovamente la Commissione sia a fornire prove valide sulla necessità della raccolta, dell'archiviazione e del trattamento dei dati PNR per raggiungere gli obiettivi dichiarati, sia ad esaminare comunque alternative meno invasive.

631 COM(2010) 492 finale, 21.9.2010, cit.

632 P7_TA-PROV(2010)0397, consultabile su http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0397+0+DOC+XML+V0//IT.

CAPITOLO TERZO
Il Garante per la protezione dei dati personali, la tutela dei dai personali ed alcune questioni ancora aperte

SOMMARIO: 1. Le Autorità amministrative indipendenti: uno sguardo d'insieme su alcune questioni ancora aperte. – 2. Il Garante per la protezione dei dati personali - 2.1. Origini e disciplina. - 2.2. Compiti. – 3. Il potere normativo del Garante per la protezione dei dati personali. – 4. La tutela dei dati personali - 4.1. La tutela amministrativa. - 4.2. La tutela giurisdizionale. – 5. Il Garante per la protezione dei dati personali ed il giudizio costituzionale - 5.1. I conflitti di attribuzione fra poteri dello Stato - 5.2. I conflitti di attribuzione fra Stato e Regioni. - 5.3. Il Garante per la protezione dei dati personali come giudice *a quo* nel giudizio costituzionale incidentale. - 6. Il ricorso pregiudiziale alla Corte di giustizia.

1. Le Autorità amministrative indipendenti: uno sguardo d'insieme su alcune questioni ancora aperte

Il Garante per la protezione dei dati personali rientra fra le cd. Autorità amministrative indipendenti. Si tratta, come noto, di un quadro molto complesso: la nascita e la posizione delle Autorità indipendenti nel nostro ordinamento è stata ed è tuttora questione controversa. Da qui, oltre al copioso dibattito dottrinale, anche i diversi tentativi, a cui si accennerà di seguito, di sistemazione e di riforma di queste figure[633].

L'analisi del fenomeno, tuttavia, non può prescindere dalla considerazione che questi enti non sono stati istituiti in aderenza ed esecuzione di un disegno legislativo omogeneo[634], sebbene abbiano come

[633] Sulla necessità di non seguire necessariamente la via delle semplificazioni unificanti e sul fatto che queste possano costituire una forzatura, vedi G. AMATO, *Autorità semi – indipendenti ed Autorità di garanzia*, in Rivista trimestrale di diritto pubblico, 1997, pag. 653; U. DE SIERVO, *Le diversità fra le varie Autorità*, in Autorità indipendenti e principi costituzionali. Atti del Convegno di Sorrento 30 maggio 1997, Cedam, Padova, 1999, pag 71.

[634] La difficoltà, quindi, di ricostruirne un quadro sufficientemente unitario ha spinto qualcuno a rinvenire la necessità di porsi di fronte alle Autorità indipendenti come dinanzi ad un dipinto impressionista, allontanando lo sguardo per coglierne i tratti complessivi. Così F. CINTOLI, *I regolamenti*

comune denominatore il fatto di nascere, anche sotto la spinta delle Istituzioni comunitarie, per soddisfare un'esigenza di regolazione di settori cd. "sensibili" della vita sociale ed economica dell'ordinamento con un più elevato grado di incidenza sulle libertà dei cittadini[635], secondo canoni improntanti sia a specifiche competenze tecniche sia ai principi di garanzia e neutralità. Questo consente loro di agire in una posizione di imparzialità, rispetto agli interessi coinvolti: cd poteri garanti[636].

Il presupposto per l'affermazione del modello incentrato sulle Autorità indipendenti è stato rinvenuto nell'esistenza di quello che è stato definito uno "spazio amministrativo sufficientemente aperto" [637]: un sistema, cioè, che a livello costituzionale garantisce al potere legislativo un margine di manovra piuttosto ampio e a quello amministrativo un'autonoma capacità di determinazione rispetto al Governo.

Si tratta, quindi, di un'amministrazione non strutturata in modo rigido ma, al contrario, tale da consentire l'adozione, per via legislativa, di soluzioni organizzative differenziate.

Inoltre, l'"erompere"[638] delle Autorità indipendenti ha rappresentato un momento significativo di un lungo e complesso processo evolutivo tutt'ora in atto nell'amministrazione, ovvero il progressivo passaggio da un modello amministrativo piramidale ad un modello policentrico e pluralistico.

L'essenza del fenomeno di queste figure è stata rinvenuta, infatti, anche nella garanzia e nell'espletamento delle funzioni di *administrative regulation*, "quale espressione di una moderna e democratica visione

delle Autorità indipendenti nel sistema delle fonti tra esigenze della regolazione e prospettive della giurisdizione; in giustizia-amministrativa.it, 2003.

635 Cfr. A PIZZORUSSO, *La Costituzione. I valori da conservare, le regole da cambiare*, Einaudi, Torino, 1996, p. 148.

636 Cfr S. CASSESE, C. FRANCHINI (a cura di), *I garanti delle regole. Le Autorità Indipendenti*, Il Mulino, Bologna, 1996; F. CARINGELLA, *La Misteriosa identità delle autorità indipendenti: pubbliche amministrazioni speciali o espressione di un quarto potere acefalo e vagamente mostruoso?*, in Lezioni e Sentenze di diritto amministrativo 2007, ildirittopericoncorsi, 2007, pag 276 e ss; riguardo alla loro natura in merito all'esercizio di poteri normativi da parte della Authorities cfr parere del Consiglio di Stato, Sez. normativa,n. 11603/05 e n. 355/2006.

637 Cfr. C. FRANCHINI, *Le autorità indipendenti come figure organizzative nuove*, in S. CASSESE, C. FRANCHINI (a cura di), I garanti delle regole, cit., p. 69; S. REGASTO, *Contributo allo studio delle Autorità Indipendenti. Il caso del garante per l'editoria e la radiodiffusione*, ARACNE editrice S.r.l., 2004, consultabile su http://www.aracneeditrice.it/pdf/690.pdf.

638 Termine usato da A. PREDIERI, *L'erompere delle autorità amministrative indipendenti*, Passigli,1997.

dell'amministrazione, non più 'braccio operativo' delle scelte compiute dalla maggioranza politica"[639].

In questo contesto, le caratteristiche principali che le pongono al di fuori del modello amministrativo tradizionale sembrano essere due: l'indipendenza e la conseguente neutralità. Quest'ultima, in particolare, non si identifica tuttavia con la terzietà, connotato della funzione giurisdizionale, ma rappresenta una sublimazione del principio di imparzialità (art 97 Cost.) in combinazione con la previsione dell'indipendenza di tali figure.

"In questo senso dire che la pubblica amministrazione, ovvero una particolare pubblica amministrazione, è terza, vuol dire che essa, ancorché provveda a soddisfare l'interesse pubblico di cui è esponente, qualificando con gli effetti dell'atto amministrativo posizioni di parti anche contrapposte e da essa considerate in contraddittorio, fa uso del principio di imparzialità"[640]

Le Autorità operano, infatti, nelle materie e nei settori di rispettiva competenza, in posizione di indipendenza dal Governo come dagli altri poteri dello Stato, gravando loro semplicemente un'attività di relazione e rendicontazione periodica nei confronti del Governo e del Parlamento.

Ancora, queste figure sono in buona parte tributarie, oltre che di funzioni propriamente amministrative, anche e soprattutto di compiti di regolazione e giustiziali. Esse, cioè, dettano regole nel settore loro affidato (almeno le Autorità di settore) e dirimono gli eventuali conflitti fra gli operatori, comminando sanzioni in caso di comportamenti non conformi alle prescrizioni normative o alle decisioni prese in sede giustiziale.

Pertanto, in ragione della collocazione nel tessuto istituzionale che sono venute assumendo, così come per le funzioni che sono chiamate a svolgere, le Autorità indipendenti suscitano diversi interrogativi sul "fondamento della loro legittimazione rispetto ai canoni correnti delle democrazie moderne" in quanto " un controllo affidato [*ndr* solamente] allo strumento giurisdizionale non risulta (…) sufficiente a trasformare una 'investitura tecnocratica' in una 'legittimazione democratica', quando entrano in gioco

[639] Così F. POLITI, *La potestà amministrativa delle Autorità amministrative indipendenti: nuovi profili di studio*, in N. LONGOBARDI, Autorità amministrative indipendenti e sistema giuridico-istituzionale, 2° ed., Giappichelli, Torino, 2009, pag 298.

[640] Corte di Cassazione, Sez. I Civile, 20 maggio 2002 n 7341, consultabile su http://www.privacy.it/cassaz20020520.html.

poteri che (…) possono assumere nella sostanza la natura di veri e propri poteri di governo"[641].

La questione della legittimazione porta a considerare, poi, l'assetto complessivo delle Autorità nel nostro ordinamento[642], nonché il problema della compatibilità costituzionale di questi organismi, difficilmente collocabili nello schema classico dei poteri dello Stato.

Di qui viene anche l'esigenza, da molti avvertita, di formalizzarne nel testo della Carta costituzionale la presenza di queste peculiari istituzioni. Infatti, da un lato ciò varrebbe a supportarne l'esistenza, dall'altro potrebbe essere utile per evitare una loro eccessiva proliferazione.

Come è stato osservato, in sintesi le proposte avanzate in tal senso possono raggrupparsi in due filoni principali "a) inserire in Costituzione una generale norma di riconoscimento per le Autorità indipendenti; b)

[641] E. CHELI, *Parlamento e autorità indipendenti*, in Associazione italiana dei costituzionalisti, Annuario 2000, Il Parlamento, atti del XV Convegno annuale Firenze 12-14 ottobre 2000, Cedam, Padova, 2001, pag.321-324. Per P. CARETTI, s tratta "un confronto tutt'altro che facile ma appunto problematico" fra "due principi diversi fra loro: quello della legittimazione democratica (solidamente ancorato al nostro impianto costituzionale) e quello della legittimazione Cfr. anche F. BILANCIA, *La crisi dell'ordinamento giuridico dello Stato rappresentativo*, Cedam, Padova, 2000, pag 13-14 e 131, il quale, come osservato da G. GRASSO in, *Le Autorità amministrative indipendenti della Repubblica*, Giuffrè, 2006, pag. 5, colloca il fenomeno delle Autorità indipendenti tra le "varianti , rispetto al circuito, di legittimazione sostenuto dalla rappresentanza politica", individuando nell'indipendenza e neutralità "i nuovi fondamenti di un sistema istituzionale, prima ancora che normativo, alternativo alla tradizione democratica".

[642] Si vedano anche le Indagini conoscitive svolte dalla svolta dalla Commissione Affari Costituzionali della Camera dei Deputati nel 2000, Presentazione, consultabile su http://leg15.camera.it/organiparlamentari/ufficiopresidenza/leg13/ _view.asp?id=128, in cui si legge: "Il tema di questa indagine conoscitiva è infatti quello di favorire, per la prima volta, a livello politico e parlamentare, una riflessione generale sulla posizione delle autorità indipendenti all'interno del sistema costituzionale. Il loro carattere indipendente non deve portare a considerarle come delle monadi, ma anzi obbliga a tenere in attenta considerazione ogni tipo di rapporto che intercorre tra di loro e tra ciascuna di esse e gli altri poteri dello Stato (…) Grazie a questa indagine conoscitiva si è ora in grado di affermare che un problema di collocazione delle autorità amministrative indipendenti all'interno di un quadro istituzionale chiaro esiste nell'ordinamento italiano e deve essere tenuto in considerazione, in primis dal legislatore, ogni qual volta intenda intervenire istituendo una nuova autorità o ritoccando i caratteri di quelle esistenti.

Si sono inoltre poste le basi per decidere se e in quali termini procedere, nel futuro, ad una disciplina delle autorità indipendenti a livello costituzionale, a livello legislativo e a livello di regolamenti parlamentari. Inoltre i frutti di questo lavoro potranno riflettersi anche nel miglioramento di singole disposizioni che interesseranno questo o quell'aspetto, questa o quella Autorità.". Gli atti relativi all'indagine conoscitiva sono stati raccolti nel volume Camera dei Deputati, *Le Autorità amministrative indipendenti*, collana Indagini conoscitive e documentazioni legislative n. 31, XIII legislatura, Roma, 2000. L'elaborazione di un testo di riforma ha continuato ad essere oggetto di dibattito anche successivamente. Nella legislatura immediatamente successive, ad esempio, il ministro per la funzione pubblica Mazzella, i ha portato all'attenzione del Consiglio dei ministri uno schema di disegno di legge recante *Norme e principi in materia di organizzazione e funzionamento delle Istituzioni pubbliche indipendenti*. Tuttavia si è mai pervenuti alla approvazione di un disegno di legge da presentare alle Camere. In questo senso si veda l'indagine conoscitiva tuttora in corso della Commissione I, Affari Costituzionali, della Presidenza del Consiglio e Interni della Camera, http://www.camera.it/558; http://www.camera.it/459?eleindag=/_dati/leg16/lavori/stencomm/01/indag/indipendenti, http://www.astrid-online.it/Riforma-de3/Atti-parla/Indagine-c/index.htm.

prevedere un'elencazione dettagliata in costituzione delle diverse autorità o meglio di quelle Autorità che meritano davvero un rango costituzionale"[643].

La prima prospettiva ha trovato riscontro prima nel progetto di riforma della Costituzionale elaborato dalla Commissione bicamerale, istituita con la Legge cost. 1/1997,[644] e più recentemente nell'art 35 della Legge di revisione costituzionale del 18 novembre 2005, recante: "Modifiche alla Parte II della Costituzione.", il quale prevedeva l'introduzione nel testo costituzionale di un art 98 bis, intitolato appunto "Autorità amministrative indipendenti nazionali"[645].

Come noto, il testo di legge costituzionale, approvato in seconda deliberazione con maggioranza inferiore a due terzi dei componenti di Camera o Senato, è stato successivamente bocciato a seguito del referendum, svoltosi il 25 ed il 26 giugno 2006[646].

Sempre ai fini della loro legittimazione, c'è poi chi ha richiamato l'elemento "politico", valorizzando la "complessa rete di rapporti" che le Autorità intrattengono con Parlamento, Governo[647].

Altri hanno individuato il fondamento costituzionale delle Autorità indipendenti dall'interpretazione del nuovo art 117 della Costituzione,

---

643 G. GRASSO, *Le Autorità amministrative indipendenti della Repubblica*, op cit. pag. 111.

644 Il progetto di revisione della Parte seconda della Costituzione (A.C. 3931-A e A.S. 2583-A). Consultabile su http://www.camera.it/parlam/bicam/rifcost/dossier/aindice.htm. Art. 109*(Autorità di garanzia e di vigilanza)*. Per l'esercizio di funzioni di garanzia o di vigilanza in materia di diritti e libertà garantiti dalla Costituzione la legge può istituire apposite Autorità. Il Senato della Repubblica elegge a maggioranza dei tre quinti dei suoi componenti i titolari delle Autorità di garanzia e di vigilanza. La legge ne stabilisce la durata del mandato, i requisiti di eleggibilità e le condizioni di indipendenza. Le Autorità riferiscono alle Camere sui risultati dell'attività svolta.

645 Gazzetta ufficiale n. 269 del 18 novembre 2005, consultabile su http://www.camera.it/EventiCostituzione2007/ cd_rom_studi/2_Testi/01_Testo_legge_cost.pdf. Art. 35. (Autorita' amministrative indipendenti nazionali). Per l'esercizio di funzioni di garanzia o di vigilanza in materia di diritti e libertà garantiti dalla Costituzione la legge può istituire apposite Autorità. Il Senato della Repubblica elegge a maggioranza dei tre quinti dei suoi componenti i titolari delle Autorità di garanzia e di vigilanza. La legge ne stabilisce la durata del mandato, i requisiti di eleggibilità e le condizioni di indipendenza. Le Autorità riferiscono alle Camere sui risultati dell'attività svolta.

1. Dopo l'articolo 98 della Costituzione, e' inserito il seguente: "Art. 98-bis. - Per lo svolgimento di attivita' di garanzia o di vigilanza in materia di diritti di liberta' garantiti dalla Costituzione e su materie di competenza dello Stato, ai sensi dell'articolo 117, secondo comma, la legge approvata ai sensi dell'articolo 70, terzo comma, puo' istituire apposite Autorita' indipendenti, stabilendone la durata del mandato, i requisiti di eleggibilita' e le condizioni di indipendenza.

Le Autorita' riferiscono alle Camere sui risultati delle attivita' svolte".

646 http://www.camera.it/EventiCostituzione2007/cd_rom_studi/5_Referendum/Ref02_Procedimento.htm

647 G. SIRIANI, *Nuove tendenze legislative in materia di amministrazioni indipendenti*, Nomos, 1993, pag. 89 e ss.; C. NARDELLI, *Il potere di nomina delle Autorità Indipendenti dei Presidenti di Camera e Senato della Repubblica italiana: un modello ormai superato*, consultabile su http://amministrazioneincammino.luiss.it/wp-content/uploads/2010/04/15795_Nardelli.pdf.

collegata alla finalizzazione delle singole autorità ad una migliore protezione di valori e diritti sanciti nella Prima parte della Costituzione[648].

Inoltre, è stato anche osservato che il modello organizzativo espresso dall'art. 95 Cost., imperniato sulla responsabilità politica del Presidente del Consiglio e dei Ministri, riguarderebbe strettamente solo l'azione del governo e non tutta l'amministrazione[649].

Di conseguenza, la disposizione costituzionale espliciterebbe essenzialmente "una sorta di imperativo ipotetico", prevedendo che "ove sia necessaria e ravvisabile una dipendenza dell'amministrazione dal governo, i membri di quest'ultimo, collegialmente o individualmente, sono chiamati a risponderne"[650].

L'art. 97 della Cost., invece, rappresenterebbe la norma di copertura sotto la quale può operare l'amministrazione, quando è chiamata a svolgere funzioni che non richiedano l'assunzione di una responsabilità politica[651].

Per altri ancora "il silenzio della Costituzione oggi preoccupa meno che ieri, poiché il ruolo delle Autorità si è consolidato, è divenuto parte integrante del diritto vivente, si è incastonato nelle maglie, fortunatamente non troppo strette della nostra Carta fondamentale"[652].

Secondo qualcuno, poi, la carenza di legittimazione politico-rappresentativa sarebbe in realtà compensata dalla previsione di forme di

[648] G. GRASSO, *Le Autorità amministrative indipendenti della Repubblica*, op cit. pag 8. Vedi anche G. AMATO, *Le Autorità indipendenti nella Costituzione economica*, in AA.VV., Regolazione e garanzia del pluralismo. Le Autorità Amministrative indipendenti, Giuffrè, Milano pag 16, secondo cui le Autorità di garanzia "se non hanno necessariamente uno spazio esplicito nella seconda parte della Costituzione, hanno un fondamento costituzionale nella seconda". Ancora G. GIACOBBE, *Competenza della Authorities e tutela dei diritti della persona*, in P. PERLINGERI (a cura di), Authorities e tutela della persona, Esi, Napoli, 1999 pag .53, il quale riconosce la loro legittimazione nel "vigente sistema costituzionale se, e nella misura in cui, esse siano preordinate alla tutela dei diritti fondamentali della persona".

[649] G. GEMMA, *Garante per la radiodiffusione e l'editoria e conflitti di attribuzione tra i poteri dello Stato*, in Giur. Cost., 1995.

[650] F. CARINGELLA, *Corso di diritto amministrativo*, Giuffrè, Milano2004, p. 885.

[651] Contra M. CLARICH, G. CORSO, V. ZENO-ZENCOVICH, *Le autorità indipendenti: un catalogo delle questioni aperte*, atti del Convengo Il sistema delle Autorità indipendenti: problemi e prospettive, Roma 27 febbraio 2006, consultabile su eprints.luiss.it/128/1/Clarich_2006_01_OPEN.pdf, i quali osservano che "Sebbene sia diffusa, sull'autorità di Mario Nigro, l'opinione che la Costituzione contenga più modelli di amministrazione – un'amministrazione servente del Governo (art. 95), un'amministrazione imparziale (art. 97) ed un'amministrazione autonomistica (art. 5 Cost.) – non vi è dubbio che l'amministrazione imparziale coincide con l'amministrazione servente di cui all'art. 95; o che al più, l'amministrazione servente è una parte di quella amministrazione imparziale che abbraccia anche l'amministrazione autonomistica. Il che esclude che l'art. 97 possa costituire fondamento sufficiente per una amministrazione indipendente:considerato che l'imparzialità convive con la funzione strumentale rispetto al governo che è prevista all'art. 95".

[652] F. CINTOLI, *I regolamenti delle Autorità indipendenti nel sistema delle fonti tra esigenze della regolazione e prospettive della giurisdizione*, op. cit.

democrazia cd. procedimentale[653], per cui le Autorità riceverebbero di conseguenza "una legittimazione democratica posteriori", in quanto "nel procedimento si contiene (…) la democraticità complessiva o l'insieme democratico dell'amministrazione"[654].

Pertanto, il procedimento partecipativo non svolgerebbe una funzione di mera razionalizzazione delle decisioni delle Autorità indipendenti, ma sarebbe anche lo "strumento della partecipazione dei soggetti interessati, sostitutivo della dialettica propria delle strutture rappresentative"[655].

In tal modo, si verrebbe anche a "colmare il deficit di legalità sostanziale"[656] delle Autorità, "sganciate in qualche misura dal circuito democratico tradizionale"[657], facendo da contrappeso ai "poteri normativi quasi in bianco"[658] spesso esercitati dalle stesse, come si vedrà più avanti.

Lo strumento partecipativo delle Autorità indipendenti risponderebbe, inoltre, alla finalità di fornire una risposta alla crisi della legge[659]. Queste figure - lo si è visto in relazione al Garante per la protezione dei dai personali - operano, in settori in cui vi è un'evoluzione tecnologica talmente rapida da rendere molto difficile al legislatore stare al passo, fornendo una disciplina organica che risulti immune da una "rapida obsolescenza"[660].

---

653 S. CASSESE, *Negoziazione e trasparenza nei procedimenti davanti alle Autorità indipendenti*, in Il procedimento davanti alle Autorità indipendenti, Quaderni del Consiglio di Stato, Torino, 1999, pag 42. Vedi anche M. MANETTI, *Profili di giustizia costituzionale delle autorità indipendenti*, in Associazione italiana dei professori di diritto amministrativo, Annuario 2002, Giuffrè, Milano, 2003, pag 229, secondo cui questa procedimentalizzazione sarebbe il "fondamento di una legittimazione autonoma, che si muove a livello costituzionale perché invera una forma di democrazia partecipativa ex art 3, comma 2, Costituzione". Contra G. GRASSO, *Le Autorità amministrative indipendenti della Repubblica*, op. cit. pag 82: "perché, per le Autorità indipendenti, la disciplina del contraddittorio e il rispetto delle norme generali della legge n. 241/90 dovrebbero avere una valenza diversa da quella delle altre amministrazioni, per le quali è la democrazia rappresentativa a fondarne previamente la legittimità, insieme ai principi costituzionali dell'imparzialità, della soggezione alla legge e del buon andamento? Delle due l'una: o le Autorità non sono amministrazioni (a tutto concedere sarebbero amministrazioni differenziate), o è la disciplina della l. n. 241/1990, applicata alle Autorità, a non risultare sufficiente, esprimendo solo <<una generica legittimazione procedurale>>, che caratterizza, a ben vedere <<tutte le istituzioni nelle moderne società complesse>>".

654 G. BERTI, *Amministrazione e Costituzione*, Dir. Amm., 1993, pag 465.

655 R. CHIEPPA, *Tipologie procedimentali e contradditorio davanti alla Autorità indipendenti*, consultabile su www.giustizia-amministrativa.it, pag 3. Vedi anche F. MERUSI, *Democrazia ed autorità indipendenti*, Mulino, 2000, pag. 27 il quale descrive il fenomeno in termini di di vera e propria "prevalenza" della legittimazione procedimentale sulla rappresentatività, riguardo ai poteri finalizzati alla tutela di posizioni di garanzia tutelate direttamente a livello costituzionale.

656 M. CLARICH, I procedimenti di regolazione, in AA.VV., Il procedimento davanti alle autorità indipendenti, Giappichelli, Torino, 1999 pag. 19.

657 M. CLARICH, *ult. op. cit*.

658 M. CLARICH, *ult. op. cit*.

659 R. CHIEPPA, *Tipologie procedimentali e contradditorio davanti alla Autorità indipendenti*, op cit., pag 3.

660 Così R. CHIEPPA, *ult. op. cit*. pag 3. Vedi anche E. L. CAMILLI, M CLARICH, *Poteri quasi giudiziali delle autorità indipendenti*, nota elaborata per il gruppo di lavoro Astrid "La riforma delle Autorità indipendenti", consultabile su http://www.astrid-online.it/Riforma-

Oltre a ciò, si è anche osservato che in relazione alla funzione giustiziale di alcune Autorità, il "potenziamento del principio del contraddittorio, nelle sue varie manifestazioni concrete, costituisce senz'altro un elemento qualificante del modello"[661].

Altri hanno sostenuto, ancora, che tali figure troverebbero la loro legittimazione nella derivazione comunitaria di molte di esse o comunque nel rafforzamento dei loro poteri prodotto dal diritto comunitario[662], quasi a "trasformare questi organismi nella *longa manus* del diritto europeo dei diritti nazionali"[663].

Secondo questa linea, l'indipendenza è "un elemento essenziale per consentire all'Unione europea di contare su tali autorità anche in un'attività di stimolo, promozione e vigilanza in ordine all'attività statuale di attuazione delle direttive di armonizzazione. L'indipendenza di tali autorità non ha un fondamento di ordinamento interno, né è una scelta dello Stato italiano, ma ha un fondamento di tipo europeo ed è un vincolo dello Stato italiano"[664].

Da quanto indicato appare chiaro che non vi è accordo sulla posizione delle Autorità indipendenti nel nostro ordinamento, così come le opinioni concernenti i poteri da queste esercitate sono diverse e spesso molto divergenti.

In questa sede, tuttavia, non è possibile, pertanto dare conto della varietà delle questioni sollevate in merito alle Autorità indipendenti, le quali, fra l'altro, sono caratterizzate da una forte disomogeneità normativa l'una dall'altra.

---

de3/Contributi/Camilli_Clarich_gruppo_AI.pdf, in cui si osserva che: " in presenza della crisi della legge come fonte di disciplina di attività private in settori dinamici e soggetti a processi di innovazione tecnologica rapidissimi, come quelli nei quali operano le autorità indipendenti, ha colpito l'attenzione degli interpreti l'ampiezza dei poteri complessivamente devoluti a quest'ultime, tanto da far dubitarne la compatibilità con i principi dello Stato di diritto e del canone della legalità e tipicità dei poteri che è fondamentale in un ordinamento democratico".

661 E. L. CAMILLI, M CLARICH, *Poteri quasi giudiziali delle autorità indipendenti,* op. cit.

662 F. MERUSI, *le autorità indipendenti tra riformismo nazionale e autarchia comunitaria*, in F. A. GRASSINI (a cura di), L'indipendenza delle autorità, Il Mulino, Bologna, 2001, pagg. 26-27.

663 G. GRASSO, *op. cit.*, pag 98.

664 "Anche la tematica, sulla quale ritornerò, che ha molto interessato i miei colleghi delle discipline costituzionalistiche italiane, sempre alla ricerca di quale sia il fondamento costituzionale dell'indipendenza delle autorità, è fuorviante, perché tale fondamento non si trova né nel quadro interno, né nel quadro costituzionale, ma in quello europeo." Così F. PIZZETTI, Presidente del Garante per la protezione dei dati personali, nell'audizione presso Commissione I, Affari Costituzionali, della Presidenza del Consiglio e Interni della Camera, in sede di indagine conoscitiva. Consultabile su http://www.astrid-online.it/Riforma-de3/Atti-parla/Indagine-c/index.htm.

Di seguito, senza alcune pretesa di completezza ci si soffermerà, quindi, in particolare sulla figura del Garante per la protezione dei dati personali - pur non escludendo comunque alcune considerazioni generali – poiché questa Autorità indipendente ha e avrà in futuro un ruolo cardine nel rapporto fra tutela della privacy e lo sviluppo delle nuove tecnologie, come si è messo in evidenza nel capitolo precedente.

2. Il Garante per la protezione dei dati personali

2.1. Origini e disciplina

Il Garante per la protezione dei dati personali è un'Autorità indipendente istituita dalla legge n. 675 del 1996.

Sin dalla sua creazione l'attività del Garante ha riguardato ogni settore della vita sociale ed economica del paese in cui si sia riscontrata l'esigenza di protezione dei dati personali. Particolarmente importanti sono stati i suoi interventi nei settori delle telecomunicazioni, della sanità, del lavoro, del giornalismo, della comunicazione, della videosorveglianza, del marketing, della genetica e delle nuove tecnologie.

Si è già rilevato, inoltre, che l'istituzione di un apposito organismo di garanzia e di controllo dell'applicazione della normativa a tutela del corretto trattamento dei dati personali ha configurato un adempimento di precisi obblighi comunitari ed internazionali.

La Convenzione del Consiglio d'Europa n. 108 del 1981[665], infatti, pur non facendo espresso riferimento ad organismi specifici, ha richiesto comunque agli Stati aderenti l'individuazione di uno o più autorità per l'applicazione su base territoriale delle relative norme pattizie nonché per lo svolgimento delle attività di cooperazione e di assistenza.

Successivamente, l'Accordo di Shengen[666] e la successiva Convenzione di applicazione hanno previsto, fra le altre cose, la creazione di un sistema informativo comune per finalità di sicurezza e di ordine pubblico. L'adesione degli Stati è stata così condizionata non solo alla previa adozione

[665]Cfr. capitolo I.

[666] Cfr. capitolo I.

di discipline nazionali di tutela del trattamento dei dati personali, ma anche la creazione di autorità di vigilanza nelle sezioni nazionali, in cui è articolato il sistema.

Oltre a ciò, come è noto, l'istituzione del Garante per la protezione dei dati personali è stata una conseguenza diretta dell'applicazione della Direttiva europea n. 95/46/CE[667]. La stessa Direttiva, in particolare, non si è limitata a stabilire la creazione di apposite autorità di controllo, ma è intervenuta direttamente su alcune caratteristiche e requisiti delle stesse. Già nelle premesse si legge, infatti, che la necessità che le autorità "agiscano in modo indipendente in ciascuno Stato membro è un elemento essenziale per la tutela delle persone con riguardo al trattamento dei dati personali"[668].

L'art. 28 della Direttiva[669], poi, pur non individuando vincoli in relazione alla collocazione istituzionale, composizione, struttura e modalità di

[667] Cfr. capitolo I.

[668] Considerando 62.

[669] Art 28. Autorità di controllo

1. Ogni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente direttiva, adottate dagli Stati membri. Tali autorità sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite.

2. Ciascuno Stato membro dispone che le autorità di controllo siano consultate al momento dell'elaborazione delle misure regolamentari o amministrative relative alla tutela dei diritti e delle libertà della persona con riguardo al trattamento dei dati personali.

3. Ogni autorità di controllo dispone in particolare:

- di poteri investigativi, come il diritto di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo;

- di poteri effettivi d'intervento, come quello di formulare pareri prima dell'avvio di trattamenti, conformemente all'articolo 20, e di dar loro adeguata pubblicità o quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento o quello di adire i Parlamenti o altre istituzioni politiche nazionali;

- del potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva ovvero di adire per dette violazioni le autorità giudiziarie. È possibile un ricorso giurisdizionale avverso le decisioni dell'autorità di controllo recanti pregiudizio.

4. Qualsiasi persona, o associazione che la rappresenti, può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali. La persona interessata viene informata del seguito dato alla sua domanda. Qualsiasi persona può, in particolare, chiedere a un'autorità di controllo di verificare la liceità di un trattamento quando si applicano le disposizioni nazionali adottate a norma dell'articolo 13 della presente direttiva. La persona viene ad ogni modo informata che una verifica ha avuto luogo.

5. Ogni autorità di controllo elabora a intervalli regolari una relazione sulla sua attività. La relazione viene pubblicata.

6. Ciascuna autorità di controllo, indipendentemente dalla legge nazionale applicabile al trattamento in questione, è competente per esercitare, nel territorio del suo Stato membro, i poteri attribuitile a norma del paragrafo 3. Ciascuna autorità può essere invitata ad esercitare i suoi poteri su domanda dell'autorità di un altro Stato membro. Le autorità di controllo collaborano tra loro nella misura necessaria allo svolgimento dei propri compiti, in particolare scambiandosi ogni informazione utile.

7. Gli Stati membri dispongono che i membri e gli agenti delle autorità di controllo sono soggetti, anche dopo la cessazione delle attività, all'obbligo del segreto professionale in merito alle informazioni riservate cui hanno acceso.

designazione, ha ribadito che esse "sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite" ed ha individuato parte di tali funzioni e dei relativi poteri, concorrendo così a delineare la loro fisionomia al di fuori dei modelli tradizionali di amministrazione[670].

In questa prospettiva è collocata anche la previsione di un principio generale di collaborazione e di cooperazione tra le diverse autorità nazionali. In tal senso, sempre a livello comunitario, si veda l'istituzione da parte dell' art. 29 della medesima Direttiva n. 95/46/CE del Gruppo europeo per la tutela delle persone con riguardo al trattamento dei dati personali[671].

Anche a livello internazionale, poi, sono numerosi gli strumenti di incontro e di collaborazione fra le diverse autorità per la definizione di standard di tutela generalmente riconosciuti: conferenze annuali, Comitati consultivi, altri organismi operanti nell'ambito del Consiglio d'Europa e dell'OCSE[672].

Nell'ambito del D.lgs. n. 196/2003, è l'art 154, 2 comma che ha incardinato l'Autorità nel contesto internazionale e comunitario, attribuendo al Garante funzioni di controllo e assistenza nel trattamento dei dati personali previsti dalla normativa sovra nazionale[673].

Con l'entrata in vigore del Trattato di Lisbona, inoltre, l'Autorità garante per la protezione dei dati personali è l'unica Autorità indipendente, basata oggi su tre disposizioni dei Trattati o aventi lo stesso valore di questi.

La prima è l'articolo 8 della Carta dei diritti fondamentali dell'Unione europea[674] , approvata come noto, a Nizza e che oggi, in virtù dell'articolo 6 del Trattato dell'Unione europea, ha lo stesso valore giuridico dei trattati[675].

---

[670] Così C. LACAVA, in C.M. BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d.lgs. 30 giugno 2003, n. 196 (<<Codice della privacy>>)*, Cedam, Padova, pag 1964.

[671] Cfr. Capitolo I.

[672] Per un quadro delle numerose attività svolte dal Garante in ambito comunitario ed internazionale si veda http://www.garanteprivacy.it/garante/doc.jsp?ID=45364.

[673] In particolare il Garante ad esempio opera nel contesto Shengen, rappresentato dall'Autorità di Controllo Comune su Sistema di Informazione Schengen (http://www.schengen-jsa.dataprotection.org); nell'archivio Europol (legge 23 marzo 1998, n 93) (http://europoljsb.ue.eu.int); nel sistema informativo doganale, di cui alla legge 30 luglio 1998, n 281 e al regolamento (CE) n. 515 del 1997; nel contesto Eurodac, per il confronto delle impronte digitali dei richiedenti asilo, con la relativa Autorità Comune di Controllo, istituita dal regolamento (CE) n 2725 del Consiglio.

[674] GUCE C 364/1 del 18.12.2000, consultabile su http://www.europarl.europa.eu/charter/pdf/text_it.pdf

[675] Versione consolidata del Trattato sull'Unione europea, GUUE C 83/13 del 30.3.2010, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:020:it:PDF.

Si già indicato nel primo capitolo che questa norma ha riconosciuto ai commi 1 e 2 ad ogni individuo il diritto alla protezione dei dati personali. "Tali dati devono essere trattati, secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica".

Il successivo comma 3 ha previsto espressamente che "il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

Particolarmente importante, ancora, nel Trattato sull'Unione europea l'articolo 39 che ha esteso alle attività di quello che era individuato come il secondo pilastro dell'Unione europea, cioè le attività di politica estera e sicurezza esterna (PESC), la protezione dei dati.

Anche questa norma ha disposto che il rispetto di tali disposizioni sia soggetto al controllo di autorità indipendenti[676].

Infine, nel Trattato sul funzionamento dell'Unione europea[677], che copre tutte le diverse attività dell'Unione, l'articolo 16, ai commi 1 e 2, ha ribadito che "ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti".

L'indipendenza dell'Autorità è stata ripresa anche dalla normativa italiana; secondo l'art. 153 del D.lgs. n. 196/03, infatti, "il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione".

[676] Art 39 Trattato sull' Unione europea. "Conformemente all'articolo 16 del trattato sul funzionamento dell'Unione europea e in deroga al paragrafo 2 di detto articolo, il Consiglio adotta una decisione che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del presente capo, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti".

[677] Versione consolidata del Trattato sul funzionamento dell'Unione europea, GUUE C 83/1 del 30.3.2010, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0001:0012:IT:PDF.

In particolare, il Garante è un organo collegiale, composto da 4 membri, eletti due dalla Camera e due dal Senato con voto limitato. La nomina del Parlamento appare finalizzata a "conseguire un'investitura ampia e integrativa, originata dal concorso delle contrapposte forze politiche che sia adeguata, in quanto a valore legittimante, alla formazione di un organo investito di competenze afferenti alla materia dei diritti fondamentali della persona e […] del pluralismo"[678]. Il procedimento di nomina si completa poi interamente nell'ambito parlamentare, non essendo necessaria alcuna altra formalizzazione[679].

I componenti sono scelti fra persone che assicurino indipendenza e riconosciuta competenza nelle materie del diritto o dell'informatica[680], durano in carica sette anni e non sono rieleggibili[681]. Il collegio nomina al suo interno il presidente, il cui voto vale doppio solo in caso di parità di voti.

Con tali previsioni, il legislatore ha mostrato di seguire un orientamento caratterizzato, riguardo alla costituzione di altre Autorità indipendenti, dall'utilizzo di formule generali che, tuttavia, rendono difficile l'individuazione in concreto dei relativi presupposti.

Per questo motivo, generalmente a tali indicazioni viene dato successivamente un effettivo contenuto da parte della legge con l'individuazione delle categorie professionali, con carattere di tipicità. In altre parole, è direttamente la norma a predeterminare un criterio di idoneità dei potenziali soggetti eleggibili alle cariche.

Nel caso del Garante per la protezione dei dati personali, invece, la legge non stabilisce requisiti soggettivi specifici, ma indica solamente criteri di massima, individuando solo la garanzia che nel collegio le diverse professionalità assicurino la compresenza di una qualificazione sia giuridica sia tecnica del collegio. Pertanto, la determinazione dei membri del collegio è rimessa interamente alla sovranità delle Camere.

---

678 R. D'ORAZIO, in GIANNANTONIO, LOSANO, ZENO-ZENCOVICH (a cura di), *La tutela dei dati personali, Commentario alla l. 675/1996*, Padova, pag 302.

679 Per l'individuazione della medesima procedura anche per la dichiarazione di decadenza, in analogia a quanto previsto per l'atto di nomina, pur nel silenzio della normativa, vedi C. LACAVA, in C.M. BIANCA, F.D. BUSNELLI (a cura di), *op. cit.*, pag 1971.

680 Art 153, comma 2 D.lgs 196/2003.

681 Art 47-quater del decreto-legge 31 dicembre 2007, n. 248, convertito, con modificazioni, dalla legge 28 febbraio 2008, n. 31, in precedenza il termine era di quattro anni con possibilità di rinnovo per altri quatto anni.

Questa scelta è stata considerata frutto della convinzione del legislatore che l'investitura parlamentare costituisca di per sé idonea e sufficiente garanzia della professionalità, oltre che di indipendenza, dei membri dell'Autorità[682].

Il comma 4 dell'art 153[683] del D.lgs. n. 196/03 ha stabilito, poi, un sistema di incompatibilità a pena di decadenza, finalizzato a garantire l'indipendenza del collegio da indebite interferenze, sulla scia di una scelta consolidata nell'esperienza delle altre Autorità. Si osserva, tuttavia, che per il Garante non è prevista l'estensione temporale del regime di incompatibilità anche per un periodo di tempo successivo alla scadenza dell'incarico.

Sempre a garanzia dell'autonomia dell'organo, le cariche del presidente e dei componenti del collegio sono disciplinate rispetto ai ruoli professionali da cui provengono e sono retribuite con una indennità di funzione commisurata, in proporzione differente, a quella delle supreme magistrature. Tuttavia, per la sua determinazione, il Codice in materia di protezione dei dati personali non rinvia più al regolamento del Garante, ma direttamente alle disposizioni del D.P.R. n 501/1998[684].

Come precedente individuato, il presidente viene nominato direttamente dal collegio. In particolare, il regolamento del Garante n. 1 /del 2000[685] ha previsto l'elezione a scrutinio segreto, con il voto di almeno tre componenti. Nel caso non sia raggiunta tale maggioranza dopo la terza votazione, è eletto presidente il componente che consegue il maggior numero di voti e, a parità di voti, il più anziano di età.

Il regolamento ha specificato, poi, le funzioni attribuite al collegio nel suo complesso e quelle attribuite al suo presidente[686].

---

682 Così R. D'ORAZIO, in GIANNANTONIO, LOSANO, ZENO-ZENCOVICH (a cura di), *La tutela dei dati personali, Commentario alla l. 675/1996*, op. cit. pag. 305. Sul punto vedi anche F. PIZZETTI, Presidente del Garante per la protezione dei dati personali, nell'audizione presso Commissione I, Affari Costituzionali, della Presidenza del Consiglio e Interni della Camera, in sede di indagine conoscitiva, cit.

683 Vedi anche il Regolamento del Garante n. 1/2000 sull'organizzazione ed il funzionamento "dell'ufficio del garante per la protezione dei dati personali", G.U. 13 luglio 2000 n. 162, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1098801.

684 Commi 5 e 6 art 153, D.n.lgs. 196/2003.

685 Regolamento n.1/2000, cit.

686 Artt. 2 e 3, Regolamento n.1/2000, cit. Art. 2. Il Garante. 1. Il Garante:a) determina gli indirizzi e i criteri generali della propria attività; b) nomina, su proposta del presidente, il segretario generale e conferisce l'incarico ai dirigenti anche generali e delle unità organizzative di primo livello;¹c) definisce gli obiettivi e i programmi da realizzare, indica le priorità, emana le direttive generali per l'azione amministrativa e la gestione e ne verifica l'attuazione, in conformità ai principi di cui all'art. 3 del decreto

Infine, l'ultimo comma dell'art 153 del Codice ha stabilito che l'Ufficio, di cui al successivo art. 156, è posto alle dipendenze del Garante.

2.2. I compiti

L'art 154 del Codice in materia di protezione dei dati personali ha individuato i compiti del Garante, il quale trova però anche in differenti disposizioni fonti di altre competenze.

Il suddetto articolo ha previsto un elenco ampio e dettagliato che va dalle funzioni di controllo a quelle interdittive, promozionali, consultive e propositive, rafforzando, così, la configurazione complessiva dell'Autorità come polo centrale intorno al quale si muove tutta la disciplina della privacy.

Il Garante dispone, perciò, di una varietà di strumenti finalizzati ad assicurare una tutela multiforme e dinamica dei dati personali, anche se nella sua attività tende, invero, a privilegiare un approccio non autoritativo, ma ispirato in linea di massima alla collaborazione ed alla persuasione, pur prevedendo la normativa, quando necessario, forti strumenti inibitori e coercitivi, nonché sanzioni sia amministrative che penali.

Un primo gruppo di compiti rientra nell'ambito della funzione generale di controllo attribuita al Garante, quale organo di vigilanza dell'attuazione della legge.

---

legislativo 3 febbraio 1993, n. 29, e successive modificazioni ed integrazioni; d) approva il documento programmatico, il bilancio di previsione ed il bilancio consuntivo; e) richiede pareri al Consiglio di Stato e ad altri organi consultivi; f) adotta il codice etico dell'ufficio e assolve ad ogni altro compito previsto dalle leggi e dai regolamenti.[*1. Così modificato dalla Deliberazione n. 5 del 26 gennaio 2005, in G.U. n. 44 del 23 febbraio 2005*].

Art. 3. Presidente e componenti 1. Il presidente è eletto dai componenti a scrutinio segreto con il voto di almeno tre componenti. Se tale maggioranza non è raggiunta dopo la terza votazione, è eletto presidente il componente che consegue il maggior numero di voti e, a parità di voti, il più anziano di età. 2. Il presidente: a) rappresenta il Garante; b) convoca le riunioni del Garante, ne stabilisce l'ordine del giorno, designa i relatori e dirige i lavori; c) promuove le liti e vi resiste relativamente agli atti di competenza propria o del collegio, ed ha il potere di conciliare e transigere;d) coordina l'attività dei componenti nei rapporti con il Parlamento e con gli altri organi costituzionali o di rilievo costituzionale, nell'attività di comunicazione pubblica, nonchè nelle relazioni con le autorità indipendenti e di vigilanza, con le pubbliche amministrazioni, con le autorità di controllo degli altri Paesi, con gli organi dell'Unione europea e del Consiglio d'Europa e con gli altri organismi internazionali. 3. Il Garante elegge un vicepresidente, che assume le funzioni del presidente in caso di sua assenza o impedimento. 4. I componenti possono essere incaricati di svolgere compiti specifici o di trattare questioni determinate.

L'Autorità deve verificare, quindi, che le operazioni sui dati personali siano conformi alla disciplina applicabile e che siano avvenute nel rispetto delle indicazioni contenute nella notificazione, fattagli da parte del titolare del trattamento, ai sensi dell'art 37 del D.lgs. n. 196/2003 (art 154, comma 1 let a)).

La notificazione costituisce, così, uno dei parametri di riferimento sulla base del quale avviene il controllo ed, in ragione di tale strumentalità, al Garante compete l'istituzione e la tenuta del registro dei trattamenti sulla base delle notifiche ricevute (art. 154, comma 1 let. l).

Come in precedenza osservato, l'art 154 ha raccordato il Garante anche a livello comunitario ed internazionale, assegnandogli funzioni di controllo o assistenza "in materia di trattamento dei dati personali prevista da leggi di ratifica di accordi o convenzioni internazionali o da regolamenti comunitari" (art 154, comma 2).

In generale, il controllo può essere effettuato sia d'ufficio che su istanza degli interessati o di un'associazione che li rappresenti, attraverso segnalazioni, reclami o ricorsi che, a differenza della legge n. 675/96, il Codice disciplina in maniera dettagliata (artt. 142 e ss).

Da un punto di vista formale, le segnalazioni indicano fatti o episodi anche generici per stimolare un controllo dell'Autorità, mentre i reclami sono diretti a denunciare un'infrazione circoscritta. Entrambi rappresentano strumenti volti ad attivare la funzione di controllo da parte del Garante, che ha l'obbligo di ricevere ed esaminare gli atti.

A differenza dei ricorsi, con cui possono esser fatti valere i diritti di cui all'art 7 del Codice, le segnalazioni ed i reclami riguardano tutte inosservanze di legge e di regolamento.

Legato, poi, alla generale attività di controllo è il potere del Garante di segnalare al titolare le misure opportune o necessarie per rendere il trattamento conforme alle disposizioni vigenti (art. 143, comma 1 lett. b e art 154, comma 1 lett. c). Tale competenza è ritenuta espressione di un potere ordinatorio preventivo strumentale alla funzione, appunto, di controllo[687].

[687] G.P. CIRILLO, *La tutela in via amministrativa del trattamento dei dati personali*, in La protezione dei dati personali, a cura di G. Santaniello, Cedam, Padova, 2005, pag. 739.

In merito, si è osservato che negli anni il Garante ha fatto un largo uso dello strumento della segnalazione nei più diversi settori e non sempre relativa al singolo caso specifico, ma per fornire un'interpretazione di alcune disposizioni della legge stessa, "fino a dettare principi e direttive di carattere generale sulla tutela della privacy, nonché indirizzi operativi per il corretto svolgimento dei rapporti tra privati e tra questi e le pubbliche amministrazioni in ordine al trattamento dei dati personali, evidenziando un ruolo fortemente dinamico"[688].

Funzionali al potere di verifica e di controllo sono i poteri di natura istruttoria, sebbene riferibili anche alla generalità dei compiti dell'Autorità. L'art 157 del D.lgs. n. 196/2003 ha attribuito al Garante il potere di richiedere informazioni e documenti, mentre il successivo art. 158 il potere di richiedere ispezioni e verifiche.

In particolare, nel 2009 sono state effettuate quattrocentoquarantanove ispezioni, quattrocentoventicinque delle quali sulla base dei programmi ispettivi semestrali disposti dall'Autorità[689].

Le linee di indirizzo dell'attività ispettiva sono stabilite, infatti, con cadenza semestrale dal Garante attraverso delibere di programmazione che indicano gli ambiti del controllo e gli obiettivi da conseguire[690]. Sulla base di tali indirizzi, l'Ufficio individua i titolari dei trattamenti da sottoporre a controllo e istruisce i conseguenti procedimenti.

Inoltre, per lo svolgimento dell'attività di controllo l'Autorità si avvale anche della collaborazione della Guardia di finanza, in applicazione del protocollo d'intesa del 2005[691].

Si evidenzia, infine, che al Garante italiano non può essere opposto il segreto di Stato (art. 160, comma 4 Codice privacy) [692].

---

688 Così C. LACAVA e L. CERRONI in C.M. BIANCA, F. D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d.lgs. 30 giugno 2003, n. 196 (<<Codice della privacy>>),* op. cit. pag . 1982.

689 Vedi Relazione 2009 del Garante su www.privacy.it.

690 Le linee generali della programmazione dell'attività ispettiva vengono rese pubbliche attraverso la *Newsletter* settimanale pubblicata sul sito www.garanteprivacy.it.

691 A tal fine la Guardia di finanza ha previsto, nell'ambito del Comando Unità Speciali, un apposito reparto, il Nucleo speciale privacy con sede a Roma, che provvede direttamente ad effettuare gli accertamenti, avvalendosi anche, ove necessario, dei reparti del Corpo territorialmente competenti. Nel 2009 in conseguenza delle ispezioni effettuate, sono state inviate all'autorità giudiziaria quarantatre informative per violazioni aventi rilevanza penale (di cui venti da parte del dipartimento attività ispettive e sanzioni dell'Autorità e ventitre da parte della Guardia di finanza), mentre sono state sono stati avviati trecentosessantotto procedimenti sanzionatori amministrativi (di cui duecentoventotto ad opera del Dipartimento e centoquaranta da parte della Guardia di finanza e altri organi accertatori). Per questi si rinvia alla dettagliata Relazione del 2009, cit.

Un altro gruppo di funzioni riguarda, poi, la competenza del Garante in ordine all'adozione di misure interdittive o coercitive, secondo quanto previsto anche dall'art 28 della Direttiva n 95/46/CE. Tali attività, in particolare, possono estrinsecarsi in due tipologie di provvedimenti: il divieto di trattamento dei dati (natura cautelare o definitiva) ed il blocco dei dati (natura cautelare) (art 154, comma 1 lett. d).

Nello specifico, questi provvedimenti possono essere adottati quando il trattamento "risulta illecito o non corretto anche per effetto della mancata adozione delle misure necessarie di cui alla lettera b) [dell'art' 143], oppure quando, in considerazione della natura dei dati o, comunque, delle modalità del trattamento o degli effetti che esso può determinare, vi è il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati" (art 143)[693]. Gli stessi rimedi sono previsti anche durante il procedimento di ricorso (art. 150).

Contro i provvedimenti di divieto di trattamento o di blocco dei dati il titolare può proporre opposizione, ai sensi dell'art. 152, al Tribunale del luogo di residenza del titolare del trattamento. L'opposizione non sospende l'esecuzione del provvedimento del Garante, tuttavia, "se ricorrono gravi motivi il giudice, sentite le parti, può disporre diversamente in tutto o in parte con ordinanza impugnabile unitamente alla decisione che definisce il grado di giudizio" (art 152 comma 5).

Un ulteriore gruppo di compiti può essere collocato nell'ambito della funzione cd. promozionale del Garante.

Fra questi rientrano quelli svolti ai fini dell'adozione dei vari codici di deontologia (art. 154, comma 1 lett. e)[694]. Anche in questo caso, la norma

692 "4. Per gli accertamenti relativi agli organismi di informazione e di sicurezza e ai dati coperti da segreto di Stato il componente designato prende visione degli atti e dei documenti rilevanti e riferisce oralmente nelle riunioni del Garante".

693 Ma vedi anche gli artt. 19 comma 2 e 39 sul potere di vietare la comunicazione di dati personali a soggetti pubblici se effettuata in violazione della legge e l'art 45 sul potere di vietare il trasferimento dei dati all'estero quando l'ordinamento dello Stato di destinazione o di transito dei tati non assicuri un livello adeguato di tutela.

694 Vedi anche l'art. 12 Codice privacy. Art. 12. Codici di deontologia e di buona condotta 1. Il Garante promuove nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, ne verifica la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto.

2. I codici sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana a cura del Garante e, con decreto del Ministro della giustizia, sono riportati nell'allegato A) del presente codice.

ha dato attuazione a quanto previsto dall'art. 27 della Direttiva n. 95/46/CE, che ha imposto agli Stati membri ed alla stessa Commissione di incoraggiare la formazione di codici di condotta volti a contribuire, in ragione della specificità settoriale, alla corretta applicazione della norma a tutela della privacy, assicurando così, in via preventiva, anche una maggiore partecipazione e responsabilizzazione degli operatori di settore.

Come già osservato, i codici sono espressione del potere di autorganizzazione negoziata delle diverse categorie, gruppi e soggetti interessati al trattamento dei dati in un determinato settore, tuttavia, sulla natura giuridica di questi atti non vi è accordo in dottrina[695].

Qui, si pone nuovamente in evidenzia il rilevo fondamentale che il Codice ha dato loro ai fini della liceità del trattamento dei dati personali, prevedendone altresì la pubblicazione nella Gazzetta Ufficiale e l'inserimento, tramite decreto del Ministero della giustizia, nell'allegato A) del Codice in materia di trattamento dei dati personali.

Nonostante il "vincolo" della previa disposizione legislativa identificativa del settore e "del caso" in cui l'intervento dell'autorità è consentito, ai sensi dell'art. 12 del Codice, il Garante può promuovere la sottoscrizione di *altri* codici non espressamente previsti per legge.

Questo, in particolare, può avvenire quando lo stesso ravvisi l'esigenza di regole di deontologia e di buona condotta per contribuire all'applicazione di disposizioni normative in settori di particolare interesse generale nei quali emergano specifiche problematiche, anche sulla base di eventuali richieste formulate nell'ambito delle categorie interessate, meritevoli di apposita considerazione, tenendo conto, in particolare, della natura dei dati o del loro trattamento o della necessità di rendere effettive le garanzie per gli interessati.

Viene, inoltre tenuta in considerazione anche l'evoluzione dei predetti settori e delle tecnologie applicate.

3. Il rispetto delle disposizioni contenute nei codici di cui al comma 1 costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici.

4. Le disposizioni del presente articolo si applicano anche al codice di deontologia per i trattamenti di dati per finalità giornalistiche promosso dal Garante nei modi di cui al comma 1 e all'articolo 139.

695 Si rinvia al Capitolo I. Per la giurisprudenza di veda, ad esempio, Corte di Cassazone, sentenza delle SS.UU., 20 dicembre 2007, n. 26810 e sentenza a SS.UU., 30 aprile 2008, n. 10875.

Per quanto riguarda, ancora, il ruolo del Garante si segnala che il 20 luglio 2006 lo stesso ha adottato uno specifico Regolamento - *Procedura per la sottoscrizione dei codici di deontologia e di buona condotta*[696].

Le motivazioni che hanno indotto a predisporre una procedura vincolante, per lo stesso Garante, per l'adozione degli atti in parola sono per lo più legate all'esigenza - citata nel preambolo del provvedimento - "(…) di dare compiuta disciplina e pubblicità alla procedura seguita dall'Autorità per svolgere" i compiti ad essa attribuiti, "tenuto conto del crescente rilievo che i codici di deontologia e di buona condotta assumono nei settori interessati ai fini della liceità e correttezza dei trattamenti dei dati personali e dell'utilizzabilità dei medesimi dati". Pertanto, quella di "consolidare tale procedura con un atto regolamentare del Garante", adottato in base all'art. 156, lett. a) del Codice, è stata sentita e descritta come una "necessità".

Dalla lettura dell'art. 2 del citato Regolamento si ricava, poi, un ampio margine decisionale che il Garante riconosce a se stesso. Infatti, alle categorie interessate sarebbe riservata la sola esplicitazione dell'istanza di attivazione, in quanto la decisione vera e propria di avviare – tramite la promozione – l'iniziativa regolativa rimane nella discrezionalità del Garante.

Una volta operata la scelta *se* dotare o meno un settore di un codice di comportamento, l'Autorità delibera l'inizio della procedura, dandone avviso a tutti i potenziali collaboratori nella costruzione del contenuto del documento, attraverso la pubblicazione della decisione in Gazzetta Ufficiale.

Tra l'altro, con tale decisione vengono anche individuati i criteri generali per la verifica del principio di rappresentatività dei soggetti, che saranno introdotti nel gruppo di lavoro volto alla stesura del codice.

Sempre alla funzione promozionale del Garante viene ricondotto il compito di diffusione della conoscenza delle norme che regolano la materia della privacy , la relativa *ratio* e le norme di sicurezza dei dati (art 154, let. h)).

Le attività di comunicazione, diffusione, ma anche di chiarificazione della disciplina sulla riservatezza costituiscono un obiettivo fondamentale

[696] Il regolamento n. 2/2006, G.U. n. 183 del 8 agosto 2006; Bollettino n. 74/luglio 2006, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1320030.

nell'attività del Garante, rispondendo all'esigenza di formare una vera e propria "cultura della privacy", la quale rappresenta, specie nel campo delle nuove tecnologie, lo strumento principale di tutela dei diritti della persona coinvolti nei diversi processi di trattamento dei dati, secondo quanto già evidenziato nel capitolo precedente.

Tale funzione si concretizza, ad esempio, nel regime di pubblicità dei provvedimenti del Garante nella Gazzetta Ufficiale ed in una diversificata strategia comunicativa messa in atto attraverso una pluralità di strumenti: assistenza, anche telefonica; comunicati e conferenze stampa, il Bollettino previsto espressamente dal Regolamento di organizzazione e funzionamento che raccoglie i provvedimenti, gli atti e i documenti principali, ancora, newsletter settimanale, sito web aggiornato, il notiziario bimestrale "*Garante privacy.it*", pubblicazioni e *dépliant* divulgativi, in grado di illustrare i diversi temi connessi alla protezione dei dati personali[697] .

Un ultimo gruppo di funzioni individuato dall'art. 154, può essere collocato genericamente nell'ambito della funzione consultiva e propositiva del Garante, nei confronti del Governo e del Parlamento. Questa comprende l'attività di segnalazione in ordine all'adozione di provvedimenti rilevanti in materia, la relazione annuale sull'attività svolta e la consultazione nella predisposizione di atti normativi e amministrativi (Art 154, comma 1 lett. f e m, comma 4)[698].

Si segnala, inoltre, l'attività di esame e valutazione delle leggi regionali, per fornire alla Presidenza del Consiglio dei ministri eventuali elementi di valutazione, al fine di un eventuale proponimento della questione di costituzionalità, ai sensi dell'art. 127 della Costituzione.

A questi compiti vanno, poi, aggiunti anche quelli di consultazione con altre autorità nazionali di controllo, nonché quelli, già richiamati, in ambito internazionale e comunitario (art 154, commi 2 e 3).

---

[697] In tema di rapporto fra privacy e nuove tecnologie, si veda ad esempio nel 2009 la già segnalata pubblicazione del *vademecum "Social network:attenzione agli effetti collaterali"*, curato dal Servizio relazioni con i mezzi di informazione e dedicato appunto al mondo delle comunità in rete. Realizzato in occasione della "*Giornata europea per la protezione dei dati personali"* del 2009, il *vademecum* è stato pubblicato anche in lingua inglese e distribuito al "*Junior 8 Summit*", il *meeting* dei giovani parallelo al G8 promosso dall'Unicef e svoltosi in Italia dal 4 al 12 luglio. L'opuscolo rappresenta una guida per aiutare sia persone alle prime armi, sia utenti più esperti, a sfruttare le potenzialità dei nuovi strumenti di comunicazione come le reti sociali, riducendo per quanto possibile i rischi per la vita privata e quella professionale. Consultabile su www.garanteprivacy.it.

[698] Si veda per un dettagli di tali attività nel 2009, la relativa Relazione, cit. In particolare si segnala come il Garante lamenti spesso da parte del Governo casi di mancata consultazione dell'Autorità.

Si è già accennato, infine, che le funzioni del Garante non si esauriscono nell'elencazione contenuta dall'art. 154, diverse disposizioni, infatti, sono fonti di ulteriori competenze.

Ad esempio, ai sensi dell'art 17 D.lgs. n. 196/2003, il trattamento di dati diversi da quelli sensibili e giudiziari che presentino nondimeno rischi specifici per i diritti e le libertà fondamentali, nonché la dignità dell'interessato è ammesso nel rispetto delle misure e degli accorgimenti prescritti dal Garante, in applicazione dei principi stabiliti nel Codice.

Inoltre, l'art. 40 del Codice ha previsto l'adozione da parte dell'Autorità di Autorizzazioni generali per i dati sensibili relativamente a determinate categorie di titolari o di trattamenti. Le Autorizzazioni generali sono pubblicate nella Gazzetta ufficiale[699].

3. Il Potere normativo del Garante per la protezione dei dati personali

Trovare un filo conduttore tra i diversi compiti assegnati al Garante non è semplice. In linea generale, tuttavia, questo può essere rintracciato nell'individuare il *modus agendi* che, nei parametri di liceità del trattamento fissati nel Codice in materia di protezione dei dati personali, consente di bilanciare l'interesse del soggetto, cui i dati si riferiscono, con la circolazione degli stessi, tutelando in tal modo i diritti e le libertà contemplati nell'art. 2 del D.lgs. n. 196/2003.

I criteri su cui deve basarsi l'attività del Garante sono spesso formulati in modo generico, "per principi e per obiettivi"[700]. Molto probabilmente questa scelta è stata fatta dal legislatore anche per garantire alla disciplina la possibilità di adattarsi al mutamento delle circostanze di fatto che, come visto, in materia di dati personali assumono una connotazione inevitabilmente dinamica[701].

---

[699] Altri poteri sono individuati dagli artt. 19, comma2, 20, comma 2, 24 comma 1 lett. g.

[700] F. CECAMORE, *L'autorità indipendente come giudice a quo nel giudizio costituzionale*, in R. BALDUZZI, P. COSTANZO (a cura di), Le zone d'ombra della giustizia costituzionale. I giudizi sulle leggi, Giappichelli, Torino, 2007, pag. 109.

[701] Fenomeno che però accomuna molte Autorità. In tal senso vedi F. CECAMORE," Suscita interesse (…), la tecnica redazionale delle norme istitutive delle Autorità indipendenti, caratterizzata dal manifestarsi per principi e per 'obiettivi'. Generalmente, infatti, le letti istitutive delle Autorità esordiscono con una enunciazione dei valori di riferimento del settore di competenza: libertà di concorrenza e tutela del mercato, diritto alla protezione dei dati personali, libertà e obiettività dell'informazione, diritto di sciopero, ecc, valori la cui concreta conciliazione con altri contrastanti non è rimessa al legislatore, ma alle stesse Autorità", *L'autorità indipendente come giudice a quo nel giudizio costituzionale*

Questa genericità fa si che l'Autorità nell'esercizio della sua attività abbia un margine di manovra rilevante. La legge istitutiva ed il successivo Codice finiscono per individuare in tal modo nel Garante il "baricentro di una tutela 'forte' dei diritti degli interessati"[702], affidandogli il ruolo di vero "centro propulsore" di un complesso meccanismo di garanzia che, come si è illustrato nel capitolo precedente, coinvolge la tutela di diversi diritti costituzionali e di interessi sia pubblici che privati, spesso potenzialmente conflittuali[703].

Inoltre, secondo quanto precedentemente evidenziato, l'Autorità non esercita i suoi compiti in un'unica forma tipica, bensì attraverso una serie di attività di natura diversa.

Perciò, a fronte dell'assenza di parametri concreti, stabiliti direttamente dal legislatore o dai regolamenti attuativi, in base ai quali operare la propria azione di controllo, è stato osservato come il Garante si sia così trovato di fronte due opzioni "o trincerarsi dietro l'oggettiva assenza di poteri determinati, e rinunciare a svolgere concretamente l'attività cui era preposto, o assumere di fatto quei poteri (..) e riempire esso stesso quei 'compiti' del tutto generici indicati dalla legge, emanando atti aventi oggettivamente un contenuto normativo, cioè contenenti regole integrative della stessa legge e innovative rispetto all'ordinamento preesistente"[704].

Si è assistito, così, "all'assunzione *de facto*, da parte del Garante, di funzioni sostanzialmente normative, nella piena ed espressa consapevolezza che tale autoattribuzione rappresentasse l'unica risposta possibile alle

, in op. cit. pag. 109. V anche S. RODOTà, secondo il quale nelle materie in cui sono direttamente in gioco diritti fondamentali, come le scelte direttamente incidenti sulla sfera della vita e del corpo, il diritto dovrebbe evitare di ripiegarsi sulla "astrattezza", preferendo invece rendere possibili analisi caso per caso dei diritti e dei valori in gioco. Ne deriva un modello di regolazione "soft" in cui la risposta giuridica è elaborata congiuntamente dal legislatore che formula regole generali, dal giudice con il suo ruolo quasi nomofilattico di garanzia dei diritti fondamentali, da autorità indipendenti che possono essere chiamate ad esprimere autorizzazioni caso per caso, da comitati tecnici che possono individuare protocolli, best practices e codici di deontologia, e lascia spazi sostanziali di esplicazione all'autonomia personale e alla solidarietà, in *La vita e le regole. Tra diritto e non diritto*, Feltrinelli, 2006. Vedi dello stesso autore *Tecnologia e diritti*, op. cit, pag158 e ss, "La stesse legge, quindi, deve assumere una flessibilità che la metta in condizioni di rispondere a situazioni diverse e variabili (…) la sua concreta attuazione richiede un'opera di adattamento affidata a soggetti diversi dal legislatore" e ancora S. RODOTà, *Tra i diritti fondamentali ed elasticità della normativa: il nuovo codice della privacy*, op. cit..

[702] Vedi G.P. CIRILLO e R. CHIEPPA (a cura di), *Le autorità amministrative indipendenti*, in Trattato di diritto amministrativo, vol. 41, Cedam, 2010 pag. 557.

[703] Così E. GROSSO, *Autorità indipendente o autorità onnipotente? Il potere normativo di fatto del Garante per la protezione dei dati personali e il principio di legalità*, in M. G. LOSANO (a cura di), La legge italiana sulla privacy: un bilancio dei primi cinque anni, Laterza, 2001, pag. 140.

[704] E. GROSSO, *ult. op. cit*., pag. 153.

esigenze di funzionamento di un meccanismo cui la legge istitutiva aveva fornito gli obiettivi, ma non gli ingranaggi"[705].

In particolare, la critica maggiore ha avuto ad oggetto soprattutto il profilo degli atti amministrativi a contenuto generale, in quanto proprio attraverso l'emanazione di tali atti che il Garante si sarebbe ritagliato una funzione paranormativa non prevista.

Infatti, il potere di rilasciare autorizzazioni al trattamento dei dati personali è stato inizialmente previsto dal legislatore solo come potere di adottare provvedimenti singolari caso per caso. Tuttavia, il Garante, resosi presto conto che molti casi potevano essere ricondotti a categorie omogenee, caratterizzate da problematiche simili, invece di adottare provvedimenti autorizzatori riferiti a singole fattispecie, ha deciso di approvare autorizzazioni generali.

Solo in seguito, invero, la legge ha attribuito la facoltà all'Autorità di rilasciare autorizzazioni generali.

Secondo questa critica, il suddetto riconoscimento legislativo, però, non è consistito affatto in un automatico conferimento da parte del legislatore di funzioni normative, pertanto, il Garante avrebbe trasformato una norma attributiva di un potere provvedimentale in una norma attributiva di un potere normativo[706].

Di conseguenza, si è sottolineato come la gran parte delle norme che dispongono principi e criteri sul trattamento dei dati sensibili finisca per provenire dal Garante.

In merito si deve osservare che questo discorso riguarda in realtà anche altre Autorità indipendenti, a cui è riconosciuta una più o meno ampia potestà regolamentare, pur se la medesima disomogeneità, evidenziata in riferimento alla fisionomia complessiva del fenomeno, emerge anche in molti aspetti riguardanti lo specifico ambito considerato.

In generale, comunque, si può osservare che l'evoluzione di queste figure ha rafforzato la tipologia dei loro atti normativi, sia per l'estrema varietà ed irritualità degli atti che si possono far risalire al potere

[705] E. GROSSO, *ult op. cit.*, pag. 153.

[706] E. GROSSO, *ult op. cit.*, pag. 162.

regolamentare nell'insieme inteso, sia per interpretazioni spesso "larghe" [707] delle funzioni normative delle Autorità indipendenti.

La dottrina, infatti, ha rintracciato, oltre ai tipici regolamenti diversi fenomeni già noti alla prassi amministrativa. In alcuni casi si ha l'adozione di atti previsti dalla legge, genericamente denominati direttive o linee guida; in altri, si hanno "deliberazioni" dotate dalle stesse Autorità del nome di istruzioni, circolari, formulari, somiglianti alle classiche norme interne, ma considerati (data la loro efficacia indubbiamente esterna) talvolta espressione del potere c.d. di *moral suasion*[708], talaltra di vero e proprio potere regolamentare[709].

Senza dimenticare, poi, le tesi che considerano normativi anche i poteri di influenza che le Autorità esercitano, tramite pareri o relazioni, sul contenuto degli atti normativi del Governo o del Parlamento[710].

Tra l'altro, considerato che è stata posta in dubbio la stessa adeguatezza di pensare atti normativi delle Autorità indipendenti solo sotto l'aspetto di fonti normative secondarie, la problematica in esame è stata ricondotta anche alla più generale questione della crisi del criterio gerarchico, nella soluzione delle antinomie tra le fonti. Da ciò deriverebbe come conseguenza l'emersione del criterio di competenza e un affievolimento nello stesso tempo del principio di legalità, non più in grado di vincolare efficacemente l'esercizio del potere normativo delle Autorità[711].

---

[707] Espressione usata da G. GRASSO, *Le Autorità amministrative indipendenti della Repubblica*, op. cit. pag . 215.

[708] Espressione di origine anglosassone con sui si indicano quegli atti volte a promuovere un comportamento o una prassi che, seppur giuridicamente non vincolanti, si impongono per l'autorevolezza di cui gode la stessa amministrazione. Cfr F. CECAMORE, *L'autorità indipendente come giudice a quo nel giudizio costituzionale*, op. cit., pag. 106.

[709] M. MANETTI, *I regolamenti delle autorità indipendenti*, in G. BRUNELLI, A. PUGIOTTO, P. VERONESI (a cura di), Scritti in onore di Lorenza Carlassare. Il diritto costituzionale come regola e limite al potere. Volume I , Delle fonti del diritto, Jovine Editore, Napoli, 2009, p. 191. Consultabile su http://www.associazionedeicostituzionalisti.it/dottrina/fontidiritto/I%20Regolamenti%20delle%20Autorita%27%20indipendenti.pdf.

[710] "E' in generale corretto considerare 'come facenti parte della fenomenologia della produzione del diritto tutte quelle attività poste in essere dalle Autorità indipendenti che conferiscono ad esse un ruolo propulsivo o consultivo nei procedimenti di elaborazione delle norme", G. GROSSO, *Autorità indipendente o autorità onnipotente? Il potere normativo di fatto del Garante per la protezione dei dati personali e il principio di legalità*,,*op cit*., pag 153, il virgolettato interno è di P. BILANCIA, *Attività normativa delle autorità indipendenti e sistema delle fonti*, in S. LABRIOLA, Le Autorità indipendenti, Giuffrè, Milano, 1999 , pag 157.

[711] Cfr G. GRASSO, *op. cit.* pag 212 ss.. "Molto spesso i 'regolamenti' delle autorità si muovono in uno spazio che non è pre-occupato da fonti di rango primario; di fatto perciò,e in questo non diversamente dai cd. regolamenti indipendenti del Governo, essi acquistano una posizione 'primaria', così S. NICCOLAI, *I Poteri garanti della Costituzione e le Autorità indipendenti*, ed. ETS, Pisa, 1996, pag 200.

Infatti, come già evidenziato, è stato rinvenuto dal un lato un "basso contenuto di predeterminazione nella legge dei contenuti dell'atto"[712] e dall'altro l'autoattribuzione da parte delle Autorità di poteri più o meno impliciti.

Pertanto, con il consolidarsi di queste figure si è posta sempre più nitidamente la questione del fondamento e dei limiti dei poteri normativi così esercitati.

La tematica travalica la possibilità di una completa trattazione in tale sede, in quanto si tratta di un aspetto specifico inserito in un discorso più ampio, sviluppatosi intorno all'accennata crisi del principio di legalità come parametro ancora valido di produzione normativa. Tuttavia, in merito, è possibile svolgere alcune riflessioni.

Una prima considerazione, riguarda il fondamento di tale "anomalo" potere regolamentare, una vola preso atto della sua esistenza.

Alcuni hanno individuato tale fondamento nella Costituzione, nello specifico nel già ricordato combinato disposto dei diritti della Prima parte con le norme riguardanti la pubblica amministrazione. Configurando le Autorità indipendenti come istituzioni di libertà, si è sostenuto così che "i poteri normativi non necessariamente dovrebbero trovare nella legge un esplicito fondamento, potendo trovare la loro legittimazione nell'assegnazione legislativa di una riserva di competenza"[713] .

Per altro verso, nel ritenere fondata e necessaria l'attribuzione alle *Authorities* di un potere regolamentare anche indipendente, è stata sottolineata la particolarità dell'attività che esse svolgono.

Le Autorità indipendenti sono, infatti, amministrazioni dotate di altissima specializzazione, deputate ad affrontare problemi di natura tecnica, la cui soluzione non può essere rimessa a strumenti di tipo meramente esecutivo. La fissazione di regole tecniche rivolte agli operatori di settore (regole che solo le stesse Autorità hanno la specifica competenza a fissare) implica, pertanto, necessariamente l'uso di un potere normativo regolamentare pieno.

[712] D. CALDIROLA, *Il diritto alla riservatezza*, Cedam, 2006.

[713] Così M.A. CABIDDU e D. CALDIROLA, *L'attività normativa della autorità indipendenti*, in Amministrare, 1-2, 2000, pag. 14 ss.

Perciò, in tali ambiti non potrebbe essere la legge ad occuparsi di una regolazione di dettaglio, né l'indipendenza delle *Authorities* correre il rischio di essere intaccata con l'assoggettamento dei regolamenti dalle stesse emanati a quelli governativi.

Ai regolamenti delle Autorità indipendenti, quindi, non sarebbe applicabile né l'art 17, comma 3 della legge n. 400/88, il quale stabilisce una sovraordinazione gerarchica tra regolamenti governativi e tutti gli altri regolamenti comunque riconducibili al potere esecutivo, né l'art 4 delle Disposizioni sulla legge in generale, il quale ha previsto che il regolamenti emanati da altre autorità non possano dettare norme contrarie a quelle dei regolamenti emanati dal Governo[714].

A ciò, inoltre, si aggiungerebbe la possibilità di rinvenire nell'art.117, comma 6 della Costituzione il fondamento di una potestà regolamentare extra governativa. La nuova formulazione del suddetto articolo, infatti, nel riferire il potere regolamentare allo Stato e non al solo Governo, sarebbe idonea a ricomprendere anche le Autorità indipendenti, costituendo "un implicito riconoscimento del pluralismo dei soggetti titolari di potestà normativa e della articolazione e ripartizione della potestà regolamentare all'interno della stessa amministrazione statale"[715], anche con una "diversità nella scala delle fonti"[716].

---

[714] Consiglio di Stato, Sez. cons. atti normativi, Ad. n. 11603/05 (parere), consultabile su www.issirfa.cnr.it/download/d438.pdf, "Il rapporto tra regolamenti delle autorità indipendenti e le tradizionali fonti subprimarie (regolamenti governativi e ministeriali) è prevalentemente disciplinato sulla base del "criterio di competenza", che si sostituisce al principio di gerarchia, in coerenza con la posizione indipendente delle entità in esame. (…) L'applicazione del principio di competenza comporta –come osservato in dottri-na –che i regolamenti delle autorità indipendenti "in virtù della competenza normativa attribuita dalla legge prevalgono nei confronti di qualsiasi altra norma emanata da fonti normative 'incompetenti', ivi compresi i regolamenti statali …"; d'altra parte, l'assoggettamento gerarchico dei poteri normativi delle autorità ai regolamenti statali, in via generale, male si concilierebbe con la stessa fisionomia 'indipendente'delle autorità, rispetto ai poteri del Governo.".

[715] G. DE MINICO, *Cambia l'oggetto del potere regolamentare delle Autorità Indipendenti a seguito della riforma del Titolo V della Parte II della Costituzione*, in Forum di Quad. cost., 2003.

[716] G. GRASSO, *Le Autorità amministrative indipendenti della Repubblica*, op. cit., pag 229 e ss. secondo il quale "si può verosimilmente sostenere che il riferimento esplicito alla potestà regolamentare dello Stato non significa soltanto ammettere , come si è già anticipato, la distribuzione della potestà regolamentare ad altri organi dello Stato in concorrenza col Governo, ma anche che i poteri regolamentari dello Stato sono capaci di esprimere una diversa intensità nella scala delle fonti". Cosi per i regolamenti governativi, il fatto che la Costituzione distingua per il Governo una potestà normativa primaria (decreti legislativi e decreti legge) e una potestà regolamentare porta a ritenere che questi debbano avere natura secondaria, mentre "per gli altri soggetti, organi ed organismi dello Stato, che fondano esclusivamente sull'art. 117, comma 6, la base costituzionale di potere normativo, non si impone affatto che le potestà regolamentare loro attribuita debba essere di grado secondario: per essi manca, infatti, come nel caso dei regolamenti governativi, la contrapposizione quasi assiologia con una potestà normativa primaria già attribuita allo stesso organo od organismo dalla Costituzione.".

In questo contesto, il ricorso alle Autorità porterebbe così a sviluppare il generale "processo di riconoscimento-istituzione di nuovi tipi di fonti, concorrenziali o riservate, imputate a soggetti ed organi istituzionali e sociali, come tali primarie al pari della legge, ma operanti in ambiti da esse predeterminati e secondo procedimenti da esse prefigurati"[717] .

La natura primaria o meno dei regolamenti posti in essere dipenderebbe, perciò, da quanto il legislatore, con le diverse leggi istitutive delle Autorità, abbia intesto "ritrarsi dalla disciplina di determinati settori o materie, limitandosi a dettare principi generali e a prestabilire i limiti della produzione normativa autonoma anche di 'valore' primario"[718].

In opposizione alle tesi fin qui esposta, si pone tutto il filone dottrinale che, invece, ha contestato ogni eventuale sconfinamento dei poteri normativi delle Autorità indipendenti dai vincoli delle leggi istitutive. Secondo questa linea, qualsiasi esercizio di potere regolamentare da parte delle stesse dovrebbe sempre rimanere subordinato alla legge e dove questo non avvenga si configurerà un'illegittimità di quel potere o della stesa legge, senza alcuna possibilità di immaginare una natura diversa dei regolamenti delle Autorità[719].

Inoltre, se la Costituzione impone riserve di legge, "queste si impongono in relazione alle Autorità indipendenti così come si impongono rispetto al potere esecutivo in generale"[720].

Questa impostazione ha trovato seguito anche nella giurisprudenza costituzionale, che, soprattutto recentemente è sembrata aver ripristinato le prescrizioni costituzionali in materia di fonti nel rango che ad esse compete.

[717] Così F. MODUGNO, *Riflessioni generali sulla razionalizzazione della legislazione e sulla delegificazione*, in Studi in onore di M. Mazziotti di Celso, Cedam, Padova 1995, pag. 206. Vedi anche dello stesso autore *Appunti dalle lezioni sulle fonti del diritto*, Giappichelli, 2002, pag. 78, in cui si ritiene "indiscutibile la mancanza di un fondamento anche indiretto (…) nella Costituzione" delle potestà normative primarie delle autorità indipendenti e si osserva l'"autolimitazione della legge, che attribuisce ad altre fonti la competenza per la normazione in certi settori" ed anche la possibilità, proprio per la mancanza di un fondamento costituzionale, di una "riappropriazione, purché organica, della materia da parte della legge" .

[718] Cosi ancora F. MODUGNO, *Riflessioni generali sulla razionalizzazione della legislazione e sulla delegificazione*, op. cit., pag 189-190. Vedi anche G. GRASSO, *Le Autorità amministrative indipendenti della Repubblica* ,op. cit, pag245 ss.

[719] Vedi fra i tanti F. SORRENTINO, *Sulle fonti del diritto*, ed. E.C.I.G., Genova 2002, pag. 143, secondo cui "non si potrebbe, senza violare l'art 70, creare con legge ordinaria altre fonti di carattere primario"; F. BILANCIA, *op. cit*., pag 331 e ss

[720] Così G. FALCON, *il "primo", il "secondo" ed il "terzo" garante*, in Mercati e amministrazioni indipendenti, F. Bassi, F. Merusi *(*A cura di), Giuffrè, Milano, 1993, pag 96.

Ci si riferisce in specie alla sent. n. 171/2007[721], in cui la Corte costituzionale ha sostenuto che "l'assetto delle fonti normative sia uno dei principali elementi che caratterizzano la forma di governo nel sistema costituzionale. Esso è correlato alla tutela dei valori e diritti fondamentali. Negli Stati che s'ispirano al principio della separazione dei poteri e della soggezione della giurisdizione e dell'amministrazione alla legge, l'adozione delle norme primarie spetta agli organi o all'organo il cui potere deriva direttamente dal popolo."

La classica giustificazione della primarietà della legge parlamentare e della riserva di legge, che ne è il corredo, sono state così ribadite nel loro significato di garanzia rispetto a "valori e diritti fondamentali". Il potere legislativo è legittimato ad godere di tale supremazia in quanto espressione della volontà popolare[722].

Il principio affermato nella sentenza ha una portata tale da ricomprendere non soltanto i rapporti fra Parlamento e Governo, in relazione alla legge di conversione del decreto-legge, ma qualsiasi legge che abiliti le potestà normative di soggetti diversi dal Parlamento.

Della medesima opinione è apparso anche il Consiglio di Stato[723] che, pur riconoscendo in capo alle Autorità indipendenti funzioni normative, tuttavia, ha ritenuto che l'attribuzione di tali poteri, per le fonti subordinate alla legge, vada individuata "sulla base del principio costituzionale di legalità. È quindi la legge ordinaria che, almeno per le fonti di livello regolamentare, può individuare siffatti poteri normativi, nel rispetto o, spesso, in attuazione dei principi della Costituzione e, ovviamente, entro i limiti delle materie di competenza statale".

Il Consiglio di Stato ha proseguito, poi, affermando che "il 'policentrismo normativo' che la legislazione italiana è venuta configurando si collega alla sempre più vasta distribuzione delle funzioni pubbliche fra

[721] Consultabile su http://www.astrid-online.it/rassegna/Rassegna-23/14-06-2007/Ccost_171_07.pdf. Per i commenti alla sentenza si rinvia a R. ROMBOLI, *Una sentenza "storica": la dichiarazione di incostituzionalità di un decreto-legge per evidente mancanza dei presupposti di necessità e di urgenza*, in Il Foro italiano, 2007, fasc. 7/8, consultabile su http://www.associazionedeicostituzionalisti.it/giurisprudenza/decisioni2/romboli/nota171_2007.html.

[722] G. U. RESCIGNO, *Sul principio di legalità*, in Diritto pubblico, 1995, 247, ss.

[723] Consiglio di Stato, Sez. cons. atti normativi, Ad. n. 11603/05 (parere), cit.. Ma vedi anche Consiglio di Stato, Sez. cons. atti normativi, Ad. n. 355/06 (parere), consultabile su http://www.dirittodeiservizipubblici.it/articoli/articolo.asp?sezione=dettarticolo&id=127.

una pluralità di soggetti, anche al di fuori dell'apparato governativo e ministeriale. (…).

Le autorità indipendenti costituiscono certamente una tipologia speciale di soggettività pubblica e, in questo senso, si tratta di soggetti che devono comunque trovare in un profilo legislativo primario la fonte attributiva del potere e i criteri di fondo che devono presiedere all'esercizio di tale potere.

La stessa introduzione, per legge, di una formula organizzativa che separi il regolatore amministrativo 'di settore' dalla dipendenza diretta dall'organo politico e che affianchi a processi di liberalizzazione o di deregolazione l'istituzione di organismi autonomi di disciplina e di vigilanza, crea un'area di interessi disciplinati comunque dal principio di legalità."[724].

Infine, secondo il Consiglio di Stato non è possibile stabilire in via generale una tipologia dei regolamenti adottati dalle Autorità indipendenti, poiché questi dipendono dalle specifiche prescrizioni della legislazione di settore . "In concreto, si tratta di verificare, caso per caso, quale sia la configurazione che effettivamente la legge abbia inteso imprimere ai poteri normativi riconosciuti all'autorità nell'ambito della potestà di regolazione."[725].

[724] Oltre che nella legge, anche il Consiglio di Stato rinviene nella Costituzione e nelle norme comunitarie il fondamento dei poteri normativi attribuiti alle Autorità indipendenti. "Se un fondamento legislativo è sempre necessario per stabilire il potere normativo delle cd. autorità indipendenti e i connessi limiti, ad esso si aggiungono (o anzi, ormai, si sovrappongono) anche una "copertura costituzionale"e/o una "copertura comunitaria"che presiedono ai vari ambiti di intervento.".

[725] Il Consiglio di Stato si è espresso anche in merito all'opportunità di sottoporre gli schemi di tali atti normativi al parere dello stesso Consiglio di Stato: " in conformità, peraltro, alla prassi vigente, in quanto, come già sottolineato da questo Consiglio (Ad. gen., parere 4/2003; Sezione per gli atti normativi, pareri 3075/04 e 1354/02), l'evoluzione della legislazione ha modificato le funzioni consultive del Consiglio di Stato sull'attività normativa. Queste possono riguardare ambiti estranei all'attività normativa del Governo statale (articolo 17, comma 28, della legge 127/97: 'La Sezione [consultiva per gli atti normativi] esamina altresì, se richiesto dal Presidente del Consiglio dei ministri, gli schemi di atti normativo dell'Unione Europea') e tendono a estendersi anche alla normativa di produzione regionale, secondo quanto previsto da vari Statuti regionali (ad es., l'articolo 40 dello Statuto della Regione Puglia), e dal D.Lgs 373/03, recante le norme di attuazione dello Statuto speciale della Regione siciliana concernenti l'esercizio nella regione delle funzioni spettanti al Consiglio di Stato, con il quale le funzioni consultive sull'attività normativa sono state conferite direttamente al Consiglio di giustizia amministrativa per la Regione siciliana.

La *ratio* sottesa alle norme in questione fa emergere la necessità di una visione unitaria dei processi di regolazione in un sistema a più livelli, nell'attuale contesto istituzionale di 'policentrismo normativo', ulteriormente accentuatosi dopo la riforma del Titolo V della Costituzione, anche in considerazione dell'avvertita esigenza di un sostegno tecnico-giuridico in posizione di indipendenza e in grado di favorire la necessaria coerenza del sistema.

Appare utile, in questa sede, rilevare la medesima esigenza anche per l'attività normativa delle autorità indipendenti.".

Quanto al significato del principio di legalità, si può ritenere che questo sia costituito da un "minimo", individuato appunto nella *previa legge*[726], e un "massimo", secondo in quale almeno in determinati ambiti o in relazione a determinati oggetti, il potere non deve soltanto fondarsi sull'esistenza di una legge, ma deve anche essere conforme nel contenuto a regole materiali previste all'interno di quella o di altre leggi. A queste ultime è richiesto di indicare gli scopi ai quali l'atto sub legislativo dove essere finalizzato, i criteri da seguire per la sua emanazione ecc.

"Tra il 'minimo' e il 'massimo' del principio di legalità si colloca l'intera problematica dei rapporti tra la legge e gli atti – sia normativi che non normativi – della Pubblica Amministrazione"[727] ed anche, come si è visto, delle Autorità indipendenti.

Sul punto si è espresso ancora il Consiglio di Stato[728], ritenendo che "se non pare possano esservi dubbi sui poteri regolamentari di organizzazione (ivi compresi quelli aventi ad oggetto il procedimento), la cui estensione dipende dal grado di autonomia che le singole leggi istitutive hanno lasciato alle autorità indipendenti, l'ambito delle altre potestà regolamentari attiene alle caratteristiche e ai poteri delle singole autorità nei confronti degli 'amministrati'.

Se la materia è analiticamente o, comunque, in buona parte disciplinata dalla legge, i regolamenti delle autorità presenteranno caratteristiche affini ai regolamenti esecutivi, di attuazione e completamento della disciplina legislativa; sul rispetto della legge si potrà incentrare il sindacato giurisdizionale.

In altri casi il potere regolamentare è attribuito alle autorità indipendenti con un mero riferimento o alla materia oggetto di regolamentazione o, al più, a concetti giuridici indeterminati o a finalità di carattere generale. In queste ipotesi, la dottrina ha parlato di regolamenti autonomi, simili a quelli che nell'ordinamento della pubblica amministrazione governativa vengono definiti indipendenti.

---

[726] Anche qui si distingue ulteriormente tra espressa previsione legislativa o riconduzione anche per via implicita del potere ad una legge.

[727] Così E. GROSSO, *Autorità indipendente o autorità onnipotente? Il potere normativo di fatto del Garante per la protezione dei dati personali e il principio di legalità,* op. cit., pag 169.

[728] Consiglio di stato, sez consult., Ad n 355/06, cit.

Su tale ultima categoria di regolamenti non è mancata qualche perplessità, essendo più evidenti i rischi di deroga al generale principio di legalità. D'altra parte la configurazione, in certi casi, di una maggiore discrezionalità delle autorità indipendenti anche nell'esercizio delle loro funzioni normative risulta coerente col loro ruolo, che non è solo quello di eseguire e dare attuazione, ma regolare e quindi anche regolamentare, in conformità alle esigenze che via via si pongono nel settore di afferenza, anche e soprattutto sulla base del dato dell'esperienza, della prassi, l'azione di quanti vi operano.

Ad avviso della Sezione, appare dunque ragionevole ammettere, in via generale, la configurabilità anche di questo tipo di regolamenti, ma ribadire la necessità di accertare, caso per caso, la sussistenza della condizione che la materia regolata non sia sottoposta a riserva di legge e che nella stessa legge istitutiva dell'autorità, o comunque in altra fonte primaria (anche di livello comunitario), siano rinvenibili i criteri di fondo per l'esercizio del potere normativo dell'autorità di regolazione."

Oltre a ciò, l'esercizio di poteri normativi da parte delle Autorità indipendenti pone problematiche particolari anche quando tali poteri siano destinati ad incidere sulle posizioni dei privati, come nel caso dell'esercizio dei poteri di controllo e sanzionatori.

In tali ipotesi, l'esercizio di poteri regolatori da parte di Autorità poste al di fuori della tradizionale tripartizione dei poteri e del circuito di responsabilità, delineato dall'art. 95 della Costituzione, è ritenuto comunque "giustificato anche in base all'esistenza di un procedimento partecipativo, inteso come strumento della partecipazione dei soggetti interessati sostitutivo della dialettica propria delle strutture rappresentative.

Secondo questa ricostruzione, come già indicato, il rischio di una caduta del valore della legalità sostanziale deve essere compensato almeno in parte con un rafforzamento della legalità procedurale, sotto forma di garanzie del contraddittorio."[729].

[729] Consiglio di stato, sez consult, Ad n 355/06 (parere), cit. "A tal fine, l'Autorità da un lato dovrà prevedere idonee garanzie partecipative in sede di approvazione dei propri regolamenti e dall'altro dovrà dotarsi di sistemi di consultazione preventiva, volta a raccogliere il contributo informativo e valutativo dei soggetti vigilati (il rapporto tra consultazione e qualità della regolazione è sottolineato anche, a livello comunitario, dal Protocollo n. 7 al Trattato di Amsterdam, in quanto una regolamentazione negoziata e concordata ha maggiori probabilità di essere accettata e quindi applicata)".

Al riguardo, è stato osservato che la possibilità di imputare alla partecipazione nel procedimento davanti alle Autorità indipendenti la capacità di rimediare "(non a monte ma a valle)"[730], almeno in parte, alla carente legalità della materia ha trovato accoglimento nel quadro del diritto positivo grazie alla legge 28 dicembre 2005 n. 262.

L'art 23 della suddetta normativa, infatti, ha previsto tre principi, a cui Banca d'Italia, Consob, Isvap e Covip debbono conformarsi nel procedere all'adozione tanto degli atti generali quanto dei regolamenti: consultazione degli interessati, motivazione, revisione periodica[731].

La partecipazione al procedimento assumerebbe così il significato di volizione concorrente dei cittadini: non si tratta di un consenso che fa venir meno la forma autoritativa dell'atto, ma che lo plasma dall'interno, con ciò attenuando l'esigenza di predeterminazione legislativa[732].

Nello specifico, poi, la partecipazione giacché rivolta ad atti di contenuto generale implicherebbe la legittimazione di tutti gli interessati e comporterebbe da parte degli stessi di prese di posizione di carattere altrettanto generale: "è insomma qualcosa di diverso dal limitato ingresso di interessi particolari quale normalmente avviene nel procedimento amministrativo, rappresentando piuttosto una discussione pubblica sull'opportunità di adottare una determinata disciplina"[733].

Quanto al principio della motivazione degli atti, questo sarebbe indispensabile per un controllo effettivo sull'atto, mentre il principio della revisione periodica sarebbe legato all'oggetto della regolazione, necessariamente dinamico.

Inoltre, il riferimento operato dalla suddetta disposizione sia ai regolamenti che agli atti amministrativi generali troverebbe giustificazione nel fatto che, come già rilevato, le Autorità indipendenti adottano spesso atti generali innominati, contenenti prescrizioni che si pretendono dotate di

730 Così M. MANETTI, *I regolamenti delle autorità indipendenti* , op. cit.

731 Secondo M. MANETTI, *I regolamenti delle autorità indipendenti,* op. cit., "Essi riuniscono quindi tutte e tre le caratteristiche che, singolarmente considerate, hanno giustificato nella prassi del nostro ordinamento la ritrazione del legislatore dalla disciplina di una materia, e la delega ad organi amministrativi".

732 così M. MANETTI, *I regolamenti delle autorità indipendenti,* op. cit.

733 "Una partecipazione così concepita sembra idonea ad integrare la disciplina legislativa, in quanto meccanismo che risponde alla medesima *ratio* : garantire che le norme siano adottate nel contraddittorio degli interessati o dei loro rappresentanti liberamente scelta", M. MANETTI, *I regolamenti delle autorità indipendenti,* op. cit.

efficacia non meramente persuasiva, ed usano talvolta atti generali al fine di integrare o modificare il disposto legislativo.

Sarebbe decisamente opportuno applicare, quindi, anche a questi ultimi il medesimo trattamento previsto per i regolamenti, assicurandone altresì la generale conoscibilità.

In sede di controllo giurisdizionale, il giudice dovrebbe verificare se l'atto abbia o no carattere normativo, al fine dell'applicazione della relativa disciplina.

In merito alla suddetta tesi, si osserva che, se è vero che quanto stabilito a livello di principi dalla legge n. 262 del 2005, può ritenersi applicabile anche all'argomento generale qui trattato, tuttavia, non sembra ravvisabile nella stessa – come è stato fatto - l'introduzione di un vero e proprio "modello nuovo e autonomo di produzione normativa basato sul rapporto dialogico tra il pubblico potere e gli interessati"[734], bensì solamente un modo diverso di espressione del principio di legalità.

Laddove, infatti, per le caratteristiche del settore oggetto di regolazione, questo principio non possa estrinsecarsi nell'individuazione stringente dei criteri sostanziali, lo stesso si espliciterà nella fissazione da parte della legge di più rigorosi criteri procedurali, che in ogni modo disciplinano l'esercizio del potere - normativo o amministrativo generale - ed hanno anche essi funzione di garanzia dei soggetti destinatari dell'atto.

Per quanto riguarda, in particolare, gli atti a contenuto generale e l'attività nel suo complesso del Garante per la protezione dei dati personali, si osserva come questa sia effettivamente improntata al principio della trasparenza, della massima partecipazione dei soggetti interessati – tramite ad esempio l'apertura di vere e proprie consultazioni pubbliche - al principio della motivazione degli atti e dalla revisione periodica degli stessi, dovuta alla dinamicità intrinseca della materia.

Infatti, come si è avuto già modo di illustrare, quello della privacy e della protezione dei dati personali rappresenta un settore trasversale inserito in un quadro globale, nazionale ed internazionale, in continuo movimento anche per l'effetto dell'incessante sviluppo tecnologico.

[734] Così come osservato da M. MANETTI, *I regolamenti delle autorità indipendenti*, op. cit., la quale definisce l'atto prodotto "nuova fonte" pur riconoscendo che "in base ai principi costituzionali, questa nuova fonte non può considerarsi né primaria, né riservataria nei confronti delle fonti primarie ; e neppure può considerarsi indipendente dall'attribuzione legislativa".

Perciò, è necessario considerare che, se è vero che la normativa (la L. n. 675/96 prima e il D.lgs. n. 296/2003 ora) ha affidato al Garante un rilevante potere di propulsione, controllo e disciplina della materia[735] e che meglio avrebbe fatto ad attribuirgli espliciti poteri normativi, limitandoli nell'oggetto e specificando, per gli aspetti soggetti a riserva di legge, i criteri e le direttive idonee a contenere in un ambito bel delimitato l'esercizio dei poteri stessi[736], è altrettanto vero che questa è una critica da rivolgere alla tecnica legislativa adoperata, più che nei confronti dell'Autorità[737].

Invero, il Garante è oggetto di innumerevoli segnalazioni da parte dei soggetti pubblici e privati per avere chiarimenti o indicazioni, soprattutto in ambiti in cui, si ripete, il progresso tecnologico pone continuamente delicatissime questioni di bilanciamento fra diritti fondamentali[738].

Nella materia della protezione dei dati personali, d'altronde, non può negarsi che in questi anni l'attività dell'Autorità abbia consentito in generale una tutela maggiore dei diritti, anche delicatissimi (vedi quando osservato in tema, ad esempio di dati genetici), dei diversi soggetti coinvolti.

Inoltre, attraverso gli atti generali il Garante non solo adempie alla funzione di controllo e di promozione della normativa sulla privacy,

[735] Poteri di cui, tra l'altro, è perfettamente cosciente lo stesso Garante. Vedi quanto affermato da F. PIZZETTI nell'audizione di fronte alla Commissione della Camera Affari Costituzionali, il 17 marzo 2010, cit. "io ho poteri devastanti: se usassi fino in fondo i poteri di cui dispongo, potrei determinare conseguenze davvero devastanti. Sicuramente ho il potere per impedire ai giudici di giudicare, perché, nel momento in cui verifico che la protezione dati nelle cancellerie relativamente ai fascicoli in molti tribunali è inadeguata, dovrei interrompere il trattamento dei dati. Oppure, potrei interrompere il trattamento dei dati nelle migliaia di strutture sanitarie nelle quali i dati sanitari non sono adeguatamente protetti. Forse potrei anche impedire il trattamento dei dati in alcune vitali banche dati di polizia, nelle quali le nostre prescrizioni sono accolte con grande entusiasmo e collaborazione. Posso, però, fare tutto ciò?" e ancora "aggiungo che la nostra autorità - la ringrazio, onorevole, perché è vero - anche a livello europeo è una di quelle che ha più poteri e se n'è conferiti di più".

[736] Sent. C. Cost. n. 4/1962, consultabile su www.giurcost.org/decisioni/1962/0004s-62.html.

[737] Così riconosce lo stesso E. GROSSO, *Autorità indipendente o autorità onnipotente? Il potere normativo di fatto del Garante per la protezione dei dati personali e il principio di legalità*, op. cit.

[738] Si veda, ad esempio, il recente Comunicato stampa del Garante del 10 febbraio 2011, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1788177, in cui in merito al caso Ruby, ribadisce che i poteri del Garante sono stabiliti dalla legge: "Occorre ricordare comunque che il Garante agisce sempre nel pieno adempimento delle funzioni assegnate dalla legge e tutela quotidianamente i diritti e la dignità di tanti cittadini comuni, specialmente minori o vittime di violenza. (…) Spetta, infine, al legislatore e solo al legislatore assicurare un quadro normativo che rafforzi sempre di più un corretto equilibrio tra tutti i diritti e gli interessi in gioco in questo complesso ambito, anche tenendo conto delle evoluzioni tecnologiche." Ma vedi anche F. PIZZETTI, Audizione Commissione Camera Affari Costituzionali, cit "il problema vero, almeno per la mia autorità, prima ancora che dai poteri che ho a disposizione, è rappresentato dal riuscire a svolgere un lavoro persuasivo, incisivo, certosino e cercare di non dare misure eccessive, accontentandosi comunque di *step* e fasi".

cercando di dare indicazioni esplicative, linee guida, ma ha provveduto direttamente ad autolimitare la propria discrezionalità[739].

Senza dimenticare, inoltre, che da contrappeso alla centralità dell'attività del Garante e ad evitare che un'autorità pensata come "indipendente" si trasformi di fatto in "onnipotente"[740] c'è ed è necessario ci sia un controllo giurisdizionale pieno su tutti i provvedimenti da questo adottati, come si vedrà più avanti.

4. La tutela dei dati personali

4.1. La tutela amministrativa

L'art 141 del Codice in materia di protezione dei dati personali (D.lgs. n. 196 del 2003) ha individuato nel reclamo, nelle segnalazioni e nei ricorsi le modalità di tutela in via amministrativa della privacy e dei dati personali, sollecitando in tal modo l'intervento del Garante.

In particolare, già dalla formulazione della disposizione indicata è possibile cogliere la separazione fra gli strumenti del reclamo e della segnalazione da una parte, rispetto a quello del ricorso, inteso quest'ultimo come rimedio con cui può essere richiesta la tutela dei diritti di cui all'art 7 del Codice.

Infatti, secondo quanto già osservato, con il reclamo e la segnalazione può essere sollevata una qualsiasi violazione della normativa sulla privacy, venendo a configurarsi una tutela prevalentemente oggettiva, che appunto consente l'attivazione della funzione di vigilanza e di controllo dell'Autorità.

Per questo la legittimazione soggettiva è più ampia rispetto al solo soggetto cui i dati ineriscono: il Codice ha utilizzato la formula aperta "interessati" e ha previsto esplicitamente la legittimazione delle associazioni rappresentative.

[739] Anche in questo caso, si tratta di un elemento ammesso dallo stesso E. GROSSO, *Autorità indipendente o autorità onnipotente? Il potere normativo di fatto del Garante per la protezione dei dati personali e il principio di legalità* ,op. cit.

[740] Così E. GROSSO, *ult. op. cit*., pag. 171.

Con il ricorso del soggetto[741] titolare dei diritti specificamente individuati dal suddetto art. 7 si instaura, invece, un vero e proprio procedimento secondo gli schemi dell'attività amministrativa contenziosa.

Anche da un punto di vista procedurale i primi due strumenti si distinguono per snellezza e semplicità, non sono soggetti ad alcun limite temporale né a preclusioni riguardanti la pendenza di un giudizio civile.

Un volta pervenuto il reclamo[742], il Garante è tenuto ad accertare che la questione sottopostagli non risulti manifestamente infondata e sussistano i presupposti per adottare il provvedimento. L'Autorità anche prima della definizione del procedimento e precedentemente all'adozione delle prescrizioni contenenti "le misure opportune o necessarie per rendere il trattamento conforme alle disposizioni vigenti" (art 143, lett. b Codice) può invitare il titolare, anche in contraddittorio con l'interessato, ad effettuare il blocco spontaneamente.

Laddove, poi, il trattamento illecito rischi di provocare un pregiudizio rilevante per uno o più interessati o si ponga in contrasto con rilevanti interessi della collettività, parrebbe evincersi la possibilità per il Garante di disporre in via cautelare il blocco od il divieto in tutto o in parte dei trattamenti, sulla falsariga di quei poteri di tutela alternativa a quella giurisdizionale, disciplinati dall'art 150 del Codice[743].

Ancora meno formale è lo strumento della segnalazione, essendo esperibile anche in assenza di notizie circostanziate. Tuttavia, poiché l'obiettivo è il medesimo di quello perseguito tramite il reclamo, ovvero stimolare l'intervento del Garante, questo giustifica l'attribuzione all'Autorità (art 144 Codice) degli stessi poteri cognitori e decisori già previsti dal precedente art. 143 del Codice.

La protezione dei dati personali, poi, ha il suo momento di chiusura nella tutela amministrativa e giurisdizionale dei diritti, di cui all'art 7 Codice. Il D.lgs. n. 196/2003 ha stabilito all'art. 145, comma 1 che l'interessato può

[741] Ai sensi dell'art 9, comma 3 del Codice: " I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione".

[742] I presupposti richiesti dall'art 142 per l'attivazione del Garante sono che nel reclamo vengano inseriti "un'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste, nonché gli estremi identificativi del titolare, del responsabile, ove conosciuto, e dell'istante".

[743] Così V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Giappichelli, Torino, 2007, pag. 679.

farli valere davanti all'autorità giudiziaria o con ricorso al Garante per la protezione dei dati personali, in via alternativa, con ciò confermando la scelta già compiuta con la precedente disciplina del 1996.

Nell'ambito dell'attività giustiziale, la particolare posizione del Garante, cioè la sua indipendenza, qui intesa come regola non solo organizzativa ma di giudizio, ha portato ad interrogarsi sulla natura di tale attività.

Sia pure con diverse sfumature, la questione è sembrata potersi ricondurre alla seguente opzione: se all'attività svolta dal Garante in relazione alla soluzione di conflitti appartenga comunque all'attività amministrativa contenziosa, oppure se l'attività dell'Autorità costituisca la manifestazione di un potere para-giurisdizionale[744].

La Corte di Cassazione ha negato invero che il Garante eserciti un'attività a carattere giurisdizionale, sottolineando che anche quando viene

[744] G.P. CIRILLO, *La tutela in via amministrativa del trattamento dei dati personali,* op. cit., pg. 724. V. LUISO, BIANCA, BUSNELLI (a cura di), Tutela della privacy, in Nuove leggi Civ. 1999, sub art 29, pg 666, " (…) il garante non è e né può essere un giudice. I suoi provvedimenti sono provvedimenti formalmente e sostanzialmente amministrativi, nonostante che siano rivolti a tutelare diritti"; D. CALDIROLA, *Il diritto alla riservatezza,* op. cit., pag 177 "non può porsi in dubbio che l'Autorità garante per la protezione dei dati personali non è terza rispetto alla controversia, visto che è deputata a vigilare sull'applicazione del Codice attraverso poteri di integrazione della disciplina e conformazione della stessa rispetto al caso singolo. Certo è dotata di autonomia e di indipendenza e l'indipendenza è più di autonomia, perché implica l'assenza di vincoli (…) richiede l'assenza di qualsiasi condizionamento, sia da parte dei poteri politico-istituzionali sia da parte dei poteri privati, ma il Garante non è soggetto estraneo rispetto agli interessi in gioco e non lo è soprattutto alla luce dell'introduzione del diritto alla protezione dei dati personali, poiché questo diritto definisce l'interesse pubblico al quale sono funzionali le prerogative assegnateli dal legislatore"; F. COSTANTINI, *Sulla natura del Garante per la protezione dei dati personali*, nota a Cassazione Civile, Sez. Ia, 20 maggio 2002, n. 7341, consultabile su http://www.filosofiadeldiritto.it/NUOVO%20ARCHIVIO/CostantiniGiur2-03%20NUOVO.htm; G.P. CIRILLO e R. CHIEPPA (a cura di), *Le autorità amministrative indipendenti*,op cit., pag 557, "La previsione di due percorsi di tutela posti in alternativa fra di loro (di cui uno affidato ad un organo che, sia pure neutrale e indipendente, non arriva ad essere un giudice nel significato costituzionale del termine) deve essere intesa in un senso compatibile con i principi che informano la materia della tutela amministrativa e giurisdizionale dei diritti, soprattutto curando di assicurare quanto più possibile un'ideale simmetria tra le due strade. La posizione di neutralità e indipendenza del Garante involge, sostanzialmente, quella terzietà tipica del giudice ed assicura che, nella funzione alternativa a quella giurisdizionale, l'organo decidente si ponga in una situazione di equidistanza dalle prospettazioni delle parti, anche quando una di esse sia una pubblica amministrazione". M. CLARICH, *Autorità indipendenti. Bilancio e prospettive di un modello*, Bologna, Mulino, 2005, 156 e ss. "diventa possibile qualificare le autorità indipendenti (o almeno alcune di esse ed in special modo, l'Autorità garante della concorrenza e del mercato) come organi 'paragiurisdizionali' (…). Invero, la natura paragiurisdizionale va riconosciuta, più che all'organo in quanto tale, ad alcune delle funzioni (non tutte) attribuite alle autorità indipendenti, funzioni che ben potrebbero essere esercitate (…)da organi giurisdizionali in senso proprio". E. L. CAMILLI, M CLARICH, *Poteri quasi giudiziali delle autorità indipendenti,* op. cit. "La dimensione "quasi-giudiziale" è particolarmente rilevante nel settore della protezione dei dati personali, nella prospettiva dell'esercizio dei poteri sanzionatori ma soprattutto in merito alle forme amministrative di tutela dei diritti scaturenti dal Codice della privacy (D. Lgs. 196/03). Il legislatore ha attribuito al Garante un ruolo centrale non solo nella vigilanza delle norme e nell'attività di repressione degli utilizzi illeciti dei dati personali, ma anche nella tutela delle situazioni giuridiche soggettive attribuite dalla legge".

investito del compito di dirimere controversie esercita una funzione amministrativa[745].

Nel dettaglio, la Corte ha osservato preliminarmente che la ricostruzione della cd. paragiurisdizionalità dell'attività del Garante, operata da parte della dottrina nella immediatezza del sorgere fenomeno delle Autorità indipendenti, è fondata sul connotato della terzietà. "Nozione che solo di recente la Costituzione ha adottato in modo espresso nel testo novellato dell'articolo 111, ma che da tempo è compresa nel lessico giuridico. Con essa si indica specificamente un carattere del giudice, che affianca quello ulteriore e diverso della imparzialità, costituito dal suo distacco, dal suo essere altro, rispetto agli interessi in conflitto."

Ciò premesso, la Corte ha proseguito, considerando che "l'ordinamento anzitutto non conosce un *tertium genus* tra amministrazione e giurisdizione, alle quali la Costituzione riserva rispettivamente, per distinguerne e disciplinarne le attività, gli articoli 111 e 97. Non vi è nel sistema costituzionale una figura di paragiurisdizionalità a sé stante, distinta dalle due predette, ma piuttosto con l'uso di tale termine descrittivo si suole diffusamente indicare organi pubblici dotati di poteri la cui collocazione ha suscitato dubbi."

L'art. 102 della Costituzione, come noto, ha previsto che la funzione giurisdizionale sia esercitata da magistrati ordinari istituti e regolati dalle norme sull'ordinamento giudiziario, vietando successivamente l'istituzione di giudici speciali straordinari.

Secondo la Cassazione può considerasi giudice solo "quel soggetto pubblico che esercitando quel tipico procedimento che è il processo giudiziario dà luogo ad una decisione su diritti suscettibili di assurgere alla

[745] Cass., sent. 30 giugno 2001 n. 8889, in Foro it., 2201, I, c 2448 ss; Cass., Sez I Civile, 20 maggio 2002, n. 7341, consultabile su http://www.privacy.it/cassaz20020520.html: "(…) non è affatto sconosciuto al sistema delle autorità indipendenti, per quanto possano essere tra loro diverse, la attribuzione di un potere decisorio su diritti soggettivi veri e propri, basato cioè sulla identificazione di posizioni giuridiche tutelate e non di valutazione semplicemente discrezionali circa la sussistenza di un interesse pubblico, e pur tuttavia la soggezione dei conseguenti atti ad un controllo giudiziario, rispetto al quale il soggetto pubblico interloquisce in modo formale (…).Il problema che ne occupa dunque è stabilire se, come il tribunale di Roma ha ritenuto, il ruolo del Garante della protezione dei dati personali che adopera il procedimento di cui all'articolo 29 della legge 675, è, per ciò stesso e per la terzietà che conseguirebbe al perseguimento di un interesse pubblico, del tutto analogo a quello del giudice nel processo, sicché il Garante sarebbe assimilabile ad un giudice di primo grado che, come si legge in sentenza, per l'appunto non persegue interessi "propri". Con la conseguenza che in considerazione di tale estraneità agli interessi in gioco non sarebbe legittimato a partecipare al giudizio successivo, recte di secondo grado." Conferma la stessa impostazione anche in riferimento al nuovo Codice in materia di protezioni dei dati personali, Cass. Civ. sez. I, 25 giugno 2004, n. 11864, in Giust. civ. 2005, f. 11, I, 2731.

definitività del giudicato, al di fuori di qualunque altro controllo da parte di altro e diverso organo o potere dello Stato".

Pertanto, se, come in questo caso, è stabilita la sottoposizione dell'atto al vaglio del giudice nei termini della domanda introduttiva del giudizio di controllo, questo solo ne esclude la natura giurisdizionale, atteso che la decisione del soggetto pubblico non può considerarsi definitiva.

Conferma di questo è stata rinvenuta dalla Corte anche nel fatto che la normativa (all'epoca della sentenza la L. n. 675/96, ora il D.lgs. n. 196/2003) ha prescritto che il tribunale adito in opposizione alla delibera del Garante provvede "anche in deroga al divieto di cui all'articolo 4 della legge 2248/1865, allegato e)".

È evidente, infatti, secondo la Corte che "la deroga non avrebbe senso, nella mens legis, se non sul presupposto della natura amministrativa dell'organo e del suo procedimento, al quale la legge, proprio in considerazione della fragilità dei diritti della persona, toglie la protezione dalla intrusione dell'Ago nella attività amministrativa, altrimenti spettante.(…)."

Pertanto, come già indicato, "dire la pubblica amministrazione, ovvero una particolare pubblica amministrazione, è terza, vuol dire che essa, ancorché provveda a soddisfare l'interesse pubblico di cui è esponente, qualificando con gli effetti dell'atto amministrativo posizioni di parti anche contrapposte e da essa considerate in contraddittorio, fa uso del principio di imparzialità."

Per questi motivi, nella citata sentenza, la Corte ha riconosciuto la legittimazione passiva del Garante nel giudizio di impugnativa di un suo atto, "per far valere davanti al giudice lo stesso interesse pubblico in funzione del quale esso è predisposto, ed in tale attività resta legato all'obbligo di imparzialità proprio perché l'interesse pubblico suddetto non gli è estraneo".

Infine, riguardo alle obiezioni sul fatto che dalla natura amministrativa delle decisioni dell'Autorità deriva l'eliminazione di un grado di giudizio di merito, essendo la decisione del giudice ordinario ricorribile solo in Cassazione, la Corte ha osservato che tale effetto non è sconosciuto al nostro ordinamento ed è "pacificamente legittimo costituzionalmente. Il doppio grado di merito, come è noto, non trova copertura in una

previsione costituzionale tant'è che la unicità costituisce un dato presente nel sistema processuale, funzionale ad esigenze di efficienza.".

Ricondotta in tal modo la natura dell'attività delle Autorità, in sede giustiziale di risoluzioni di conflitti, nell'ambito dell'attività amministrativa contenziosa, tuttavia, si osserva che il procedimento delineato dagli art 145 e ss. del Codice in materia di protezione dei dati personali appare connotato da elementi comunque molto simili a quelli che caratterizzano il ricorso davanti all'autorità giudiziaria e che, nel complesso, lo stesso sembra esser stato predisposto dal legislatore per assicurare una tutela in tempi rapidi, tenendo al contempo in considerazione la rilevanza della situazione soggettiva in oggetto.

Molto probabilmente questo è anche il motivo per cui è stato confermato il principio dell'alternatività tra il rimedio amministrativo e giurisdizionale, nonostante i dubbi che in proposito sono stati sollevanti sulla sua legittimità costituzionale, anche in considerazione di quanto argomentato dalla Corte Costituzionale sul ricorso straordinario al Capo dello Stato[746] .

Inoltre, la nuova disciplina, benché abbia risposto in generale alle critiche sollevate in merito alla precedente normativa, attraverso la ricezione di tutte le disposizioni regolamentari incidenti sul diritto di difesa, tuttavia non ha affrontato la questione della facoltà del controinteressanto di chiedere la trasposizione della controversia, instaurata davanti al Garante, in sede giurisdizionale.

Al riguardo, qui si anticipa l'opinione, condivisa, di chi ha evidenziato la sostanziale identità del sindacato del giudice ordinario quando il suo intervento sia richiesto direttamente oppure avvenga in sede di opposizione avverso il provvedimento espresso o tacito del Garante. Nel caso di ricorso al Garante da parte dell'interessato, quindi, la possibilità di richiedere l'intervento al giudice ordinario sarebbe solamente spostata nel tempo, e non lederebbe il diritto di difesa dei soggetti controinteressati[747].

[746] Vedi C. Cost. 1 febbraio 1964 n. 1 in Giur. It. 1964, I, 1, c. 394 e ss., consultabile su http://www.giurcost.org/decisioni/1964/0001s-64.html.

[747] F. FIGORILLI, *La tutela amministrativa*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), op. cit. pag. 683; F.P. LUISO, *Tutela della privacy*, in C.M. BIANCA, F.D. BUSNELLI, (a cura di), in Nuove leggi civ., 1999, sub art 29, pag. 669 e ss.; D. CALDIROLA, *op. cit.*, pag. 165.

Quanto all'atto introduttivo del procedimento in sede amministrativa, questo è stato ritenuto inquadrabile fra i ricorsi amministrativi non impugnatori, poiché non è necessaria la presenza di un atto amministrativo, il che non esclude, però, che questo possa in concreto esserci (se una delle parti è una pubblica amministrazione), ma in tal caso questo viene in rilievo come fatto costitutivo della fattispecie lesiva[748].

La possibilità di ricorrere, inoltre, al Garante è subordinata al cd. interpello preventivo del titolare o del responsabile del trattamento, ai sensi dell'art 146 del Codice, salva la sussistenza di un pregiudizio grave ed irreparabile.

L'art 147, invece, ha disciplinato la modalità di presentazione del ricorso ed il suo contenuto. E' stato previsto, poi, un esame preliminare del ricorso da parte del Garante che accerta, ai sensi del successivo art. 148, l'ammissibilità dello stesso, disponendo quando necessario e possibile l'eventuale regolarizzazione.

Successivamente, l'Autorità provvede a comunicare il ricorso al titolare entro tre giorni dalla ricezione (art 149, comma 1 del Codice), invitandolo ad esercitare entro dieci giorni dal suo ricevimento la facoltà di comunicare al ricorrente e all'Ufficio la propria eventuale adesione spontanea.

In questo caso, viene dichiarato il non luogo a procedere (art 149, commi 1 e 2 del Codice), in caso contrario prende avvio il procedimento in contraddittorio fra le parti (art. 149 comma 3 del Codice). Queste possono essere rappresentate da un procuratore speciale, hanno diritto di essere sentite e facoltà di presentare memorie e documenti, mentre il Garante può disporre, anche d'ufficio, l'espletamento di una o più perizie.

Ai sensi dell'art 150, comma 1 del Codice, lo stesso può adottare le misure cautelari del blocco in tutto o in parte di taluno dei dati, ovvero l'immediata sospensione di una o più operazioni del trattamento. Il provvedimento cautelare è impugnabile unitamente alla decisione che definisce il ricorso.

Il procedimento può concludersi con un provvedimento di rigetto o di accoglimento. In tal caso, oltre all'accertamento della fondatezza della pretesa, la decisione del Garante contiene anche l'indicazione del

[748] G.P. CIRILLO, *La tutela in via amministrativa del trattamento dei dati personali*, op. cit., pag 733; F. FIGORILLI, *La tutela amministrativa*, pag 684.

comportamento che l'autore della lesione dovrà tenere. Per questo, il procedimento può essere ascritto alla categoria del procedimento sanzionatorio esecutivo e la decisione di accoglimento qualificata come ordine prescrittivo o repressivo[749].

Accanto alla possibilità di decidere espressamente sul ricorso, il Codice ha confermato la precedente scelta di mantenere l'ipotesi di silenzio-diniego[750], in caso di inerzia dell'Autorità (art. 150, comma 2 del Codice).

Avverso il provvedimento espresso o tacito del Garante, l'interessato o il titolare possono proporre ricorso al giudice ordinario (art 152 del Codice).

In merito alla fase di opposizione, in questa sede sembrano opportune alcune considerazioni.

Come si è rilevato in precedenza, la compatibilità costituzionale dei rilevanti poteri attribuiti al Garante così come della scelta di un modello di tutela amministrativa alternativa sono stati ricondotti anche al presupposto dell'impugnabilità dei provvedimenti dell'Autorità, di fronte ad un organo giurisdizionale.

Tuttavia, la possibilità di richiedere l'intervento del giudice può rappresentare un rimedio dai contenuti di fatto molto differenti, a seconda che si interpreti tale strumento come un riesame della situazione sostanziale già sottoposta all'attenzione del Garante, oppure come semplice accertamento di eventuali vizi contenuti nella decisione adottata da quest'ultimo.

Orbene, com' è stato osservato, il rinvio operato dall'art 151 del Codice alla disciplina generale contenuta nel successivo art. 152, contenente le regole del procedimento e dei poteri cognitori nonché decisori del giudice

[749] G.P. CIRILLO, *La tutela in via amministrativa del trattamento dei dati personali*, op. cit., pag 743 ess; F. FIGORILLI, *La tutela amministrativa*, pag 689 e ss.

[750] Parla di silenzio- rigetto G.P. CIRILLO, *La tutela in via amministrativa del trattamento dei dati personali*, op. cit., pag. 746; Contra F. FIGORILLI, *La tutela amministrativa*, op. cit. pag 692, per il quale "Sebbene questo appaia il criterio ermeneutico[silenzio-diniego] largamente prevalente in sede di commento della nuova (così come della precedente) disciplina, una critica va rivolta all'approccio atecnico seguito dal legislatore laddove afferma che 'la mancata pronuncia sul ricorso, decorsi sessanta giorni dalla dati di presentazione, equivale a rigetto. Ed invero, parrebbe a prima vista doversi escludere l'impiego della nozione di silenzio rigetto, in quanto è del tutto assente il collegamento gerarchico tra lì Autorità decidente e colui che popone il ricorso, elemento questo che farebbe propendere per la diversa qualificazione in termini di silenzio-diniego dell'inerzia osservata in conformità a quanto previsto ex art. 150, 2 comma del Codice" Tale conclusione è motivata anche dal fatto che "l'equiparazione dell'inerzia ad una manifestazione di volontà espressa priva del tutto gli interessati delle garanzie insite nell'obbligo di motivazione, correlata all'emanazione delle determinazioni dei pubblici poteri. Da qui, una forte limitazione del diritto di difesa del titolare – o dell'interessato – che intendano proseguire la controversia in sede giurisdizionale ex art 151 del Codice , risultando di fatto non censurabili (se non in via meramente presuntiva) i presupposti di fatto e di diritto che hanno dato luogo al rigetto del ricorso".

ordinario, parrebbe andare al di là della valenza semplicemente impugnatoria dell'opposizione[751]. Si eviterebbero così le possibili ripercussioni sul piano della legittimità costituzionale della scelta operata del legislatore, trattandosi, infatti, di dare adeguata tutela ai diritti individuati dall'art 7 del Codice.

Senza dimenticare, inoltre, che una diversa interpretazione potrebbe incidere anche sulla validità del modello che demanda, come visto, solo agli interessati la scelta tra rimedio in via amministrativa o in sede giurisdizionale, senza alcuna possibilità di trasposizione da parte del titolare o del responsabile del trattamento.

4.2. La tutela giurisdizionale

L'art. 152 del Codice al primo comma ha previsto la giurisdizione del giudice ordinario su tutte le controversie che riguardano, comunque, l'applicazione delle disposizioni dello stesso Codice in materia di protezione dei dati, comprese quelle inerenti ai provvedimenti del Garante o alla loro mancata adozione.

Questa scelta, che si è posta come eccezione rispetto alle altre Autorità indipendenti, per le quali è stata riconosciuta, invece, la giurisdizione esclusiva del giudice amministrativo, si giustifica soprattutto per il fatto che in materia di protezione dei dati personali ci si trova di fronte a diritti soggettivi di estrema rilevanza quali i diritti di personalità[752].

[751] Così F. FIGORILLI, *La tutela amministrativa*, op. cit. pag. 697; vedi anche F.P. LUISO, *Tutela della privacy*, op. cit., pag. 678-679, sebbene in riferimento alla normativa precedente.

[752] Sulla base dell'articolo 152, comma 1, del Codice, in seguito ai ricorsi proposti per l'annullamento dei provvedimenti del Garante, gli organi di giustizia amministrativa hanno dichiarato l'inammissibilità per difetto di giurisdizione del giudice amministrativo: es. TAR Lazio, Sezione Prima, 701/2007; TAR Lazio, Sezione Prima, 2664/2007, confermata dal Consiglio di Stato, Sezione Sesta, 5091/2007. Medesimo risultato per i ricorsi straordinari al Presidente della Repubblica che sono stati considerati inammissibili in conformità ai pareri del Consiglio di Stato i quali sottolineano, come avviene per l'ipotesi di cui all'articolo 152 del Codice, che "qualora la giurisdizione e la competenza dell'A.G.O. stessa (ovvero di altre Autorità giurisdizionali) sia qualificabile come esclusiva e funzionale (anche per la specificità e peculiarità del rito), è stata costantemente esclusa la possibilità del ricorso straordinario al Presidente della Repubblica avverso atti dell'Amministrazione riconducibili a tali particolari forme di tutela giurisdizionale"(così Consiglio di Stato, Sezione Prima, 4468/2007; allo stesso modo Consiglio di Stato, Sezione Prima, 3754/2008, dopo aver ricordato che in linea di principio è ammissibile una tutela concorrente sia del ricorso straordinario al Presidente della Repubblica che dell'azione di fronte al giudice ordinario avverso atti amministrativi illegittimi anche delle authorities. Il precedente orientamento espresso da Consiglio di Stato, Sezione Prima, 2265/2005, nonché Consiglio di Stato, Sezione Prima, 1735/1997, aveva ritenuto ammissibile un ricorso straordinario su un provvedimento del Garante in quanto rimedio amministrativo previsto nei confronti di atti amministrativi definitivi, a prescindere dall'attribuzione di una materia ad una determinata giurisdizione, salvo esclusione ad opera di un'esplicita norma legislativa. Adesso, tuttavia, l'articolo 7, comma 8, del codice del processo amministrativo stabilisce che "il ricorso straordinario e' ammesso

Tuttavia, si precisa che le controversie sul personale del Garante rientrano nella giurisdizione del giudice ordinario in materia di pubblico impiego contrattualizzato ex articolo 63, comma 1, del decreto legislativo 30 marzo 2001, n. 165, mentre per la materia dell'accesso ai documenti amministrativi la tutela giurisdizionale è attribuita agli organi della giustizia amministrativa, in base ad un richiamo espresso alla disciplina di cui alla legge 7 agosto 1990, n. 241 (e successive modificazioni), ad altre disposizioni di legge in materia e ai relativi regolamenti di attuazione (articolo 59 del Codice).

Inoltre, si evidenzia che in un ricorso contro il silenzio rifiuto serbato dal Garante di fronte ad un'istanza del titolare, diretta ad ottenere il provvedimento di carattere generale (art. 10, comma 8 del Codice), inerente al limite massimo per il contributo spese ottenibile dall'interessato (art. 10, comma 7 del Codice), il giudice amministrativo ha accolto il ricorso, ordinando al Garante di attivare il procedimento amministrativo di fissazione della tariffa per il contributo, invece di dichiararne l'inammissibilità per difetto di giurisdizione ex articolo 152, comma 1, del Codice[753].

In seguito, nonostante l'oggetto del giudizio riguardasse chiaramente l'applicazione di una disposizione del Codice (articolo 10, commi 7 e 8), ed in particolare la mancata adozione di un provvedimento del Garante, il Consiglio di Stato ha respinto l'appello del Garante, ritenendo in contrasto con l'articolo 103, comma primo, Cost. una lettura dell'articolo 152, comma 1, del Codice "nel senso della introduzione di una giurisdizione esclusiva nei riguardi del giudice ordinario estesa agli interessi legittimi"[754].

unicamente per le controversie devolute alla giurisdizione amministrativa"). Dalla relazione del 2009 del Garante si evince che analogamente a quanto accaduto nel 2008, nel corso del 2009 l'Autorità non ha avuto notizia di ricorsi concernenti il trattamento dei dati personali proposti avanti al giudice amministrativo.

[753] TAR Lazio, Sezione Seconda, 587/2009. E' utile sottolineare che il rito speciale contro l'inerzia della pubblica amministrazione è esperibile nelle sole ipotesi in cui sussiste la giurisdizione del giudice amministrativo in ordine al rapporto sostanziale: Consiglio di Stato, Sezione Quinta, 3974/2002; Consiglio di Stato, Sezione Quinta, 497/2004, ritiene inoltre che il difetto di giurisdizione non può essere aggirato azionando il meccanismo del silenzio rifiuto; Consiglio di Stato, Sezione Quinta, 1116/2009 statuisce altresì che "l'istituto del silenzio va infatti configurato come strumento diretto a superare l'inerzia dell'amministrazione pubblica nell'emanazione di un provvedimento amministrativo, a fronte di una posizione di mero interesse legittimo in capo al privato".

[754] Consiglio di Stato, Sezione Sesta, 5198/2009, consultabile su www.giustizia-amministrativa.it.

Secondo la Relazione del Garante per la protezione dei dati personali[755], contro tale sentenza è stato proposto ricorso in Cassazione.

Tornando al procedimento davanti al giudice ordinario, il Codice sembra aver fatto venire meno il procedimento camerale a cui la disciplina previgente rinviava.

Il legislatore, infatti, tenendo conto delle forti riserve avanzate dalla dottrina e dalla giurisprudenza sulla compatibilità del giudizio camerale nella sua configurazione tradizionale in relazione alla tutela dei diritti[756], ha optato per un rito speciale, in grado di contemperare le esigenze di speditezza, legate alla situazione soggettiva sottostante, con quelle di garanzia di tutela dei diritti soggettivi.

Per tutte le controversie, anche per quelle di opposizione alle decisioni del Garante, l'azione va proposta con ricorso depositato nella cancelleria del Tribunale del luogo di residenza del titolare del trattamento. Ai sensi dell'art 152, 3 comma del Codice, il giudice decide in ogni caso in composizione monocratica, questo ad ulteriore conferma del superamento della collegialità della decisone, legata direttamente alla cameralità del rito.

Sotto il profilo dell'istruzione probatoria si sottolineano i rilevanti poteri attribuiti all'organo giurisdizionale, in quanto, ferma la necessità di rispettare il principio del contraddittorio, questo ha la possibilità di ammettere qualsiasi mezzo di prova (art. 152, comma 9 del Codice).

Per quanto riguarda la tutela cautelare si evidenzia che, con riferimento all'opposizione ai provvedimenti del Garante, la proposizione del ricorso non sospende l'esecuzione degli stessi; tuttavia, il giudice, sentite le parti può disporre diversamente in tutto o in parte con ordinanza.

---

[755] Relazione 2009, cit.

[756] Vedi la libertà del ricorso alla tutela camerale (anche dei diritti) riconosciuta al legislatore dalla Corte costituzionale. Cfr., a es., l'ordinanza. 26 febbraio 2002, n. 35, in *Foro it.*, 2002, I, 1290 ss., con nota di A. PROTO PISANI, in cui si ribadisce che "la procedura camerale, quando sia prevista senza l'imposizione di specifiche limitazioni del contraddittorio, non viola di per sé il diritto di difesa e l'adottarla in vista dell'esigenza di speditezza e semplificazione delle forme processuali è una scelta che solo il legislatore, avuto riguardo agli interessi coinvolti, può compiere e che sfugge al sindacato di questa corte, salvo che non si risolva nella violazione di specifici precetti costituzionali e non sia viziata da irragionevolezza". Ma vedi anche A. PROTO PISANI, *Usi e abusi della tutela camerale (appunti sulla tutela giurisdizionale dei diritti e sulla gestione di interessi devoluta al giudice)*, in Riv. Dir. Civ. 1990, pag. 393. G. ARIETA, *Art. 29*, in La tutela dei dati personali. Commentario alla l. n. 675/1996, diretto da E. GIANNANTONIO, M.G. LOSANO e V. ZENO ZENCOVICH, Padova, Cedam, 1997, pag. 382; F. PICCALUGA, *L'inadeguatezza del modello camerale alla luce del novellato art. 111 cost.* - nota ad App. Genova, ord. 4 gennaio 2001, In Giust. Civ., 2002, Vol. 52 c. 1383.

Quest'ultima, poi, è impugnabile solo con la decisione che definisce il giudizio, ciò significa, forse poco opportunamente, che sarà sindacabile solo in sede di legittimità, vista la non appellabilità delle decisioni (art. 152 comma 5).

Sempre riguardo la tutela cautelare, il giudice in caso di pericolo imminente di un danno grave ed irreparabile può emanare con decreto i provvedimenti opportuni anche inaudita altera parte, fissando in un termine non superiore a quindici giorni una nuova udienza, in cui sentite le parti provvederà con ordinanza a confermare, modificare o revocare i precedenti provvedimenti (art. 152 comma 6).

Ai sensi del comma 7 dell'art 152 del Codice il decreto di fissazione dell'udienza (da ritenere unitamente al ricorso, anche nel silenzio della norma[757]) deve essere notificato su istanza del ricorrente alle altre parti ed al Garante. Questa disposizione opera sia in caso di ricorso diretto all'autorità giudiziaria sia in caso di opposizione alla decisioni del Garante, in virtù del generale richiamo effettuato dall'art 151.

Perciò, oggi è indubbio che il Garante è chiamato a partecipare anche al giudizio instaurato avverso i provvedimenti dallo stesso emanati[758].

Come prima osservato, la sentenza che definisce il giudizio, in merito o in rito, non è appellabile, ma è ammesso ricorso in Cassazione (art. 152, comma 13 del Codice). In particolare, per quello che riguarda il contenuto delle sentenze di merito si rileva la previsione secondo cui il giudice può decidere anche in deroga al divieto di cui all'art. 4 della legge n. 2248/1865, allegato E, in base al quale, come noto, al giudice ordinario non è concesso l'annullamento degli atti amministrativi.

La suddetta deroga è stata oggetto di numerose discussioni in passato, poiché la legge precedente la collocava solo nell'ambito della disciplina

[757] Così R. GIORDANO, *La tutela giurisdizionale*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Il codice del trattamento dei dati personali, op. cit., pag 713.

[758] Conformemente a quanto già dedotto dalla Giurisprudenza di legittimità durante la previgente normativa. V Cass. 20 maggio, 2002, n. 7341, cit. Contra F.P. LUISO, *Tutela amministrativa e giurisdizionale*, in F.D. BUSNELLI, (a cura di), Commento alla legge 31 dicembre 1996, n. 675, in Nuove leggi civ. comm., 1999, pag. 679. Quanto agli interventi nei giudizi relativi all'applicazione del Codice, nella Relazione del 2009 del Garante si legge che "il Garante ha limitato la propria attiva presenza, nei giudizi che non coinvolgono direttamente pronunce dell'Autorità, ai soli casi in cui sorge, o può sorgere, la necessità di difendere o comunque far valere particolari questioni di diritto. In questo quadro, l'Autorità ha seguito con attenzione tutti i contenziosi nei quali non ha ritenuto opportuno intervenire, chiedendo alle avvocature distrettuali dello Stato di essere comunque informata sullo svolgimento delle vicende processuali e di ricevere comunicazione in merito agli esiti.", cit.

dell'opposizione alle decisioni del Garante e non nella competenza generale del giudice in materia.

Al riguardo, il legislatore del D.lgs. n. 196/2003 ha chiarito che la previsione può essere utilizzata dal giudice "quando è necessario in relazione all'eventuale atto del soggetto pubblico titolare o responsabile", con ciò avallando l'interpretazione estensiva, secondo cui il Tribunale non solo potrà annullare i provvedimenti del Garante, ma anche gli eventuali atti amministrativi ad esso presupposti[759].

Sempre sul merito della sentenza, l'art 152, comma 12 del Codice ha prescritto genericamente che il giudice dispone sul risarcimento del danno, ove richiesto. Diversamente, l'art 29 della L n. 675/96 sanciva la risarcibilità del danno non patrimoniale "anche nelle ipotesi di violazione dell'art 9"[760].

Il riferimento generico operato oggi dal legislatore, tuttavia, non mette in dubbio la possibilità per il giudice di provvedere sul risarcimento del danno sia patrimoniale che non patrimoniale, secondo quanto espressamente previsto dall'art 15[761] ed in considerazione dei mutamenti giurisprudenziali in merito.

In particolare, qui si evidenziano le conclusioni alle quali è recentemente pervenuta la Corte di Cassazione[762], che ha identificato il danno non patrimoniale, di cui all'art. 2059 Codice civile, come quello determinato dalla lesione di interessi inerenti la persona non connotati da rilevanza economica, composto in categoria unitaria non suscettibile di suddivisione in sottocategorie.

Tale danno è tutelato in via risarcitoria, in assenza di reato ed al di fuori dei casi determinati dalla legge, solo quando si verifichi la lesione di specifici diritti inviolabili della persona, ossia in presenza di "un'ingiustizia costituzionalmente qualificata." Dunque, è necessario tenere conto

[759] Così R. GIORDANO, *La tutela giurisdizionale*, in in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), op. cit., pag. 719 ; M. GRANIERI, *La tutela dei diritti sulla normativa sul trattamento dei dati personali: un bilancio provvisorio*, relazione tenuta all'incontro di studi promosso dal Consiglio Superiore della Magistratura e dal Garante per la protezione dei dati personali sul tema "La protezione dei dati sei anni dopo la legge 675/1996: il nuovo codice della privacy e l'attività giudiziaria", Roma, 2-3 ottobre 2003, consultabile su http://appinter.csm.it/incontri/relaz/9412.pdf.

[760] Il quale conteneva i principi in ordine alla raccolta ed ai requisiti dei dati personali.

[761] secondo cui il danno non patrimoniale derivante da illecito trattamento dei dati personali è risarcibile come quello patrimoniale.

[762] Cass. sez. un., sentenza 11 novembre 2008, n. 26975; Vedi anche Cass. Sez. un. civili, sentenza 15 gennaio 2009, n. 794, consultabile su http://www.altalex.com/index.php?idnot=44520.

dell'interesse leso e non del mero pregiudizio sofferto o della lesione di qualsiasi bene giuridicamente rilevante.

Viste le considerazioni svolte in ordine alla rilevanza del diritto alla privacy ed alla protezione dei dati personali sarebbe difficilmente contestabile il risarcimento anche del danno non patrimoniale.

5. Il Garante per la protezione dei dati personali ed il giudizio costituzionale

Del rapporto fra Autorità indipendenti e Carta costituzionale si è già avuto modo di accennare all'inizio di questo capitolo. Tale rapporto è stato visto sia in termini di compatibilità costituzionale di un modello che si è venuto affermando, anche sotto la spinta del diritto comunitario, sia in termini di rinvenimento di una loro legittimazione nelle norme costituzionale, in particolare nei diritti provvisti nella Prima parte in rapporto con il nuovo art. 117 Cost., sia infine per un'eventuale revisione costituzionale che in vario modo le preveda espressamente.

Si è messo in evidenza, poi, che l'esercizio di alcuni poteri da parte delle Autorità ha posto ulteriori interrogativi sulla loro collocazione istituzionale, anche in rapporto ai tradizionali poteri dello Stato.

Sul punto, in particolare, da più parti è stato richiesto un intervento della stessa Corte costituzionale che "ne accerti la legittimità, il ruolo e il rango nel nostro ordinamento: un elemento di 'pubblica certezza' che non può provenire dal dibattito scientifico , nel quale si fronteggiano opinioni, o dal solo esame della legislazione vigente, che può essere illegittima"[763].

I canali attraverso cui sono stati prospettati i possibili incontri fra le Autorità indipendenti e la Corte Costituzionale possono essere diversi: i conflitti di attribuzione, il ricorso incidentale con le Autorità in veste di

[763] S. NICCOLAI, *Quando nasce un potere*. In Giur. Cost, 1995, pag 1679; vedi anche G. GRASSO, *Le Autorità amministrative indipendenti della Repubblica*, op. cit., in particolare pag. 251 e ss. "il ricorso per conflitto di attribuzioni può rappresentare un rilevante strumento per definire le controversie tra le Autorità e gli altri poteri dello Stato, nonché un insostituibile mezzo per legittimare la posizione delle Autorità nell'ordinamento costituzionale"; F. DURANTE, *La legittimazione delle autorità indipendenti ad essere parte nei conflitti di attribuzione*, consultabile su http://www.ambientediritto.it/dottrina/Dottrina%202004/legittimazione_autorita_indipendenti_durante.htm, "La legittimazione delle Autorità indipendenti a partecipare ai conflitti d'attribuzione rappresenterebbe un efficace strumento, tra i tanti possibili, di un "controllo diffuso", per contemperare la responsabilità con l'indipendenza".

giudice *a quo*[764]. Ad essi sono dedicate considerazione che seguono, tenendo conto soprattutto della figura del Garante per la protezione dei dati personali.

5.1. I conflitti di attribuzione fra poteri dello Stato

L'art. 134 della Costituzione, come noto, ha assegnato alla Corte Costituzionale il compito di giudicare "sui conflitti d'attribuzione tra i poteri dello Stato e su quelli tra lo Stato e le Regioni, e tra le Regioni".

A sua volta, la legge 11 marzo 1953, n. 87, riguardo al conflitto tra poteri dello Stato, ha previsto all'art. 37 che, "ferme le norme vigenti per le questioni di giurisdizione", esso "è risoluto dalla Corte costituzionale se insorge tra organi competenti a dichiarare definitivamente la volontà del potere cui appartengono e per la delimitazione della sfera di attribuzioni determinata per i vari poteri da norme costituzionali".

A seguito di tale accertamento, secondo l'art. 38 della medesima legge, la Consulta "risolve il conflitto sottoposto al suo esame dichiarando il potere al quale spettano le attribuzioni in contestazione e, ove sia stato emanato un atto viziato da incompetenza, lo annulla".

Nell'ottica di un'eventuale partecipazione delle Autorità indipendenti e nello specifico del Garante per la protezione dei dati personali ai conflitti di attribuzione, la prima ipotesi da verificare è la possibilità di assegnare loro la natura di poteri dello Stato.

La tematica relativa alla nozione di potere dello Stato richiederebbe per la sua ampiezza un approfondimento che esula da questa sede. Tuttavia, qui si osserva come, in un ordinamento ed in una Costituzione improntati al pluralismo istituzionale, non sia invero possibile ricondurre i poteri alla tripartizione classica – legislativo, esecutivo e giurisdizionale – quantomeno intesi nella loro dimensione soggettiva.

La nozione di potere, indicata dall'art. 134 Cost. e tracciata dall'art. 37 della L. n. 87/1953, si estende in realtà "fino a ricomprendere tutti i

[764] Quanto all'ipotesi di impugnare davanti alla Corte costituzionale atti delle Autorità, riconoscendo ad alcuni di essi la forza ed il valore di legge si rinvia a G. GRASSO, *Le Autorità amministrative indipendenti della Repubblica*, op. cit., pag. 300 ess.. Sulla possibilità di dare agli atti delle Autorità valore di norma primaria si rinvia, invece, alle considerazioni già esposte in merito ai poteri normativi delle Autorità indipendenti.

soggetti cui sia riconosciuta e garantita una quota di attribuzioni costituzionalmente definita"[765].

"Le parti" del conflitto fra poteri non sono perciò nominativamente individuabili, ma rappresentano un concetto, in cui possono trovare posto diverse strutture istituzionali, quando nell'esercizio delle funzioni loro attribuite dalla Costituzione, anche in senso lato, entrano in contrasto con altre per la delimitazione delle reciproche sfere di incompetenze.

E' evidente come in quest'ambito assuma una rilevanza particolare il lavoro svolto dalla Corte costituzionale, nell'enucleare di volta in volta le caratteristiche dei soggetti idonei ad essere qualificati come poteri dello Stato.

Per quanto riguarda, in particolare, le Autorità indipendenti, i giudici costituzionali hanno escluso dalla cerchia dei poteri dello Stato due di queste: il Garante per la radiodiffusione e l'editoria e l'Autorità per le garanzie nelle comunicazioni, succeduta alla prima con L. n. 249/1997.

Le pronunce in oggetto sono le ordinanze nn. 118 e 226 del 1995[766] e l'ordinanza n. 137 del 2000[767] e sono stata emanate tutte e tre nella fase di delibazione di ammissibilità del conflitto (art 37 comma 3 della L. n. 87/1953) - su ricorsi promossi dai comitati promotori di referendum abrogativi contro atti delle due Autorità - in relazione alla comunicazione politica e alla parità di accesso ai mezzi di informazione, contro atti del Governo e della Commissione parlamentare per l'indirizzo generale e la vigilanza dei servizi radiotelevisivi.

In particolare, nella prima ordinanza, la n. 118/95, in realtà la Corte non ha esaminato la questione della qualificazione soggettiva del Garante per la radiodiffusione e l'editoria come potere dello Stato, limitandosi a dichiarare l'inammissibilità del ricorso per "la palese inidoneità dell'atto (…) a ledere la sfera di attribuzioni dei ricorrenti".

Al contrario, nella successiva ordinanza n. 226/95, pur non soffermandosi sul fenomeno generale delle Autorità indipendenti e sulla

[765] R. ROMBOLI, E. MALFATTI, S. PANIZZA, *Giustizia costituzionale*, Giappichelli, Torino, 2007.

[766] In Giur. Cost. 1995, rispettivamente pagg. 942 e ss. e pagg. 1658 e ss, consultabili su http://www.giurcost.org/decisioni/1995/0118o-95.htm e http://www.giurcost.org/decisioni/1995/0226o-95.htm.

[767] In Giur. Cost. 2000, pagg. 1321 e ss., consultabile su http://www.giurcost.org/decisioni/2000/0137o-00.html

loro collocazione all'interno dell'ordinamento, i giudici costituzionali hanno ritenuto che le attribuzioni del Garante "disciplinate dalla legge ordinaria (v. art. 6 legge 6 agosto 1990, n. 223, e successive modificazioni e integrazioni), non assumono uno specifico rilievo costituzionale ne' sono tali da giustificare - nonostante la particolare posizione di indipendenza riservata all'organo nell'ordinamento - il riferimento all'organo stesso della competenza a dichiarare in via definitiva la volontà di uno dei poteri dello Stato".

Alla stessa conclusione la Corte costituzionale è arrivata anche nell'ordinanza n. 137/2000, in cui ha dichiarato inammissibile il ricorso nei confronti dell'Autorità per le garanzie nelle comunicazioni, in quanto questa "benché goda di una posizione di particolare indipendenza all'interno dell'ordinamento, esercita attribuzioni disciplinate dalla legge ordinaria, prive - al pari di quelle svolte dal preesistente Garante per la radiodiffusione e l'editoria al quale è succeduta - di uno specifico rilievo costituzionale, quindi non idonee a fondare la competenza della medesima a dichiarare definitivamente la volontà di uno dei poteri dello Stato"[768].

Muovendo dalle suddette pronunce, vengono in evidenza alcune considerazioni, riguardanti, da una parte, le ragioni sui cui poggiano le decisioni della Corte e la possibilità di una loro riconsiderazione e, dall'altra, se le medesime conclusioni siano estensibili alle altre Autorità indipendenti, in particolare al Garante per la protezione dei dati personali.

Così, quanto al fatto che il Garante per la radiodiffusione e l'editoria sia disciplinato da legge ordinaria, è stato osservato che vi sono già organi cui la Corte ha riconosciuto la natura di poteri dello Stato, pur non essendo esplicitamente previsti in Costituzione: ad esempio l'Ufficio centrale per il referendum, di cui alla l. n. 352/1970[769].

[768] Vedi in senso critico G. GRASSO, *Le Autorità amministrative indipendenti della Repubblica*, op. cit., pag 261, in cui l'autore lamenta che "portare le Autorità indipendenti nell'arena dei conflitti poteva anche essere prematuro in quegli anni, ma negare un ruolo costituzionale al Garante e, per analogia, ad altre Autorità significa(va) trascurare, a tacere d'altro, il fortissimo elemento fattuale dell'ingresso prepotente delle Autorità nel sistema costituzionale dei poteri (…). Poi la Corte avrebbe potuto anche sostenere l'illegittimità di questa formula organizzativa, ma quella era davvero l'occasione per farlo".

[769] Vedi G. GRASSO, *Le Autorità amministrative indipendenti della Repubblica* , op. cit., pag. 263.

Fin dalla sent. n. 69/78[770] la sua legittimazione, infatti, è stata rinvenuta dai giudici costituzionali nel fatto che la funzione di controllo da questo esercitata avesse almeno implicitamente una base costituzionale[771].

In particolare, l'esistenza di un fondamento anche implicito dell'Autorità si sarebbe dovuta cercata nella migliore protezione di un valore costituzionale o di un diritto specifico. La Corte avrebbe dovuto, in altre parole, svolgere "un'approfondita analisi del rapporto fra il valore costituzionale di riferimento e le caratteristiche delle competenze e della struttura impressa a tali autorità dal legislatore" [772].

A questa tesi, però, è stato obiettato che anche se le funzioni delle varie Autorità "sono riconducibili (ma non sempre) ai principi costituzionali, in quando volte alla tutela ed allo sviluppo di valori costituzionali, non può dirsi che la loro assenza determini un *vulnus* in organi costituzionali o di rilevanza costituzionale" e che anche se "appare sicuramente stonato che organi di garanzia così significativi e rilevanti (…) siano privi di accesso al conflitto (e, di converso, non siano soggetti passivi di conflitti per il loro sconfinamento)", questo non elude "l'ostacolo dell'assenza di canonizzazione in sede costituzionale, sia dello *status* di indipendenza, sia delle funzioni di rilievo costituzionale", non potendosi creare poteri in via interpretativa[773].

[770] http://www.giurcost.org/decisioni/1978/0069s-78.html.

[771] R. ROMBOLI, E. MALFATTI, S. PANIZZA, *Giustizia costituzionale*, op. cit..

[772] Così L. CASETTI, *la cultura del mercato fra interpretazioni della Costituzione e principi comunitari*, Giappichelli, Torino, 1997, pag. 353. ; Vedi anche G. LOMBARDO, *Le autorità amministrative indipendenti come poteri dello Stato nei conflitti di attribuzione*, in Quad. cost. 1998, pag. 290., secondo cui benché le autorità non siano riconosciute espressamente dalla costituzione "i territori in cui operano (…) trovano un preciso riscontro costituzionale" e che "le leggi istitutive di queste autorità sono leggi ordinarie, ma si tratterebbe, in realtà, di attuazione di principi costituzionali, un dato che inciderebbe in modo sostanziale sull'aspetto formale della potenziale 'revocabilità' della legge stessa". Ancora, si veda M. MANETTI, *Profili di giustizia costituzionale delle autorità indipendenti*, op. cit., pag. 226, secondo la quale ci possono essere organo "non presenti in Costituzione, che si muovono, almeno sotto certi profili, a livello costituzionale". S. STAMMATI, *Tre questioni in materia di "autorità amministrative indipendenti"*, in in Associazione Italiana dei Costituzionalisti, Autorità indipendenti e principi costituzionali, Cedam, Padova, 1999,pag. 84, il quale definisce le Autorità come "*organi costituzionalmente rilevanti*, o, eventualmente, *organi amministrativi di garanzia costituzionalmente garantiti*, assistiti, cioè da una garanzia costituzionale individuale di esistenza e di funzionamento indipendente", con la conseguente possibilità non solo di essere qualificati come poteri dello Stato in sede di conflitti di attribuzione, ma anche di "sollevare questioni di legittimità costituzionale".

[773] G. MORBIDELLI, *Sul regime amministrativo delle Autorità indipendenti*, in A. PREDIERI (a cura di), Le autorità indipendenti nei sistemi istituzionali ed economici, Passigli Editore, Firenze, 1997, Vol. I, pag. 145 e ss.; Così anche G. DE MINICO, Antistrust E Consob. Obiettivi e funzioni, Cedam, Padova, 1997, nota 139: "le attribuzioni delle Autorità non [sono] disegnate nel testo costituzionale, né si possono desumere in via implicita".

Invero, una cosa è ammettere che le diverse Autorità operano con poteri rilevanti ed in posizione di indipendenza, in settori in cui sono presenti sicuramente diritti costituzionalmente previsti e garantiti, e che l'attività ad esse ricondotta è funzionalizzata (spesso espressamente) dal legislatore alla tutela di questi diritti, altra cosa, però, è riconoscere nella Costituzione un vincolo per il legislatore, nell'attuare la garanzia dei suddetti diritti attraverso le Autorità indipendenti.

Semmai il fatto che la loro attività provveda efficacemente alla tutela di così rilevanti posizioni giuridiche qualifica la loro istituzione come costituzionalmente possibile (e finanche auspicabile). Tuttavia, non tutto ciò che è legittimo da un punto di vista costituzionale, può per questo essere automaticamente considerato anche costituzionalmente necessario ed in questo caso riservato.

Se la Corte costituzionale ritenesse necessari da un punto di vista costituzionale tali organismi solo per queste ragioni, con ogni probabilità imporrebbe un vincolo al legislatore che non le è dato porre.

Né d'altronde sembra idonea la riforma del titolo V della Costituzione, in particolare l'art 117 nella parte relativa alla redistribuzione delle competenze fra Stato e Regioni, a fornire una diversa qualificazione delle Autorità indipendenti .

Infatti, voler ricavare dal fatto che "alcuni classici *domaines sensibile* affidati alla regolazione delle Autorità indipendenti risultano esplicitamente costituzionalizzati" che lo siano anche le stesse Autorità, forse rischia di far dire troppo ad un articolo che, nei commi 2 e seguenti si occupa delle competenze legislative dello Stato e delle Regioni, ma nulla dice in merito alla scelta del legislatore di affidare o meno tali settori ad Autorità indipendenti.

Nondimeno, quello che non può esser chiesto di fare alla Corte costituzionale, sulla base degli argomenti accennati, potrebbe invece essere rintracciato nel primo comma dell'art 117 Cost., laddove questo impone allo Stato ed alle Regioni il rispetto "dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali".

Orbene, restringendo a questo punto l'attenzione sulla figura del Garante per la protezione dei dati personali, si è precedentemente osservato che con l'entrata in vigore del Trattato di Lisbona, questa figura risulta ora prevista

da due norme dei Trattati ed una avente lo stesso valore giuridico di questi: l'art 8 della Carta sui diritti fondamentali dell'Unione europea, l'art 39 del Trattato sull'Unione europea e l'art 16 del Trattato sul funzionamento dell'Unione europea.

Tutte e tre le suddette disposizioni hanno stabilito che al controllo del rispetto della normativa comunitaria, volta alla tutela del diritto alla protezione dei dati personali (normativa di cui, si ricorda, è diretta applicazione anche il Codice in materia di protezione dei dati personali), deve essere preposta un'Autorità indipendente.

Senza dimenticare che, come visto, l'istituzione di tale figura, la previsione della sua indipendenza e di alcuni suoi poteri erano già richiesti dalla Direttiva n. 95/46/CE.

La "riserva di competenza" e l'indipendenza di questa Autorità, quindi, sono espressione di un preciso obbligo comunitario nei confronti dello Stato. E' perciò il diritto comunitario ad interviene sulla discrezionalità del legislatore nazionale.

Tramite l'art. 117, stavolta comma 1 e l'art. 11[774] della Costituzione questa riserva di competenza così come l'indipendenza dell'ente potrebbero, poi, assumere un indiretto rilievo costituzionale.

Quello che la Corte Costituzionale potrebbe essere chiamata allora a fare è la verifica che tale obbligo comunitario non si ponga in contrasto con i principi fondamentali del nostro assetto costituzionale[775].

In questo senso sì, avranno rilevanza le argomentazioni, precedentemente illustrate, che evidenziano come l'attività dell'Autorità sia volta ad una più efficace difesa di diritti previsti nella Costituzione e che, quindi, nel nostro ordinamento tale modello organizzativo sia da ritenersi costituzionalmente possibile.

---

[774] Fra le molte, si veda Sent. n. 348/2007, consultabile sul http://www.giurcost.org/decisioni/2007/0348s-07.html: "Questa Corte ha chiarito come le norme comunitarie 'debbano avere piena efficacia obbligatoria e diretta applicazione in tutti gli Stati membri, senza la necessità di leggi di ricezione e adattamento, come atti aventi forza e valore di legge in ogni Paese della Comunità, sì da entrare ovunque contemporaneamente in vigore e conseguire applicazione eguale ed uniforme nei confronti di tutti i destinatari' (sentenze n. 183 del 1973 e n. 170 del 1984). Il fondamento costituzionale di tale efficacia diretta è stato individuato nell'art. 11 Cost., nella parte in cui consente le limitazioni della sovranità nazionale necessarie per promuovere e favorire le organizzazioni internazionali rivolte ad assicurare la pace e la giustizia fra le Nazioni".

[775] "Con l'adesione ai Trattati comunitari, l'Italia è entrata a far parte di un 'ordinamento' più ampio, di natura sopranazionale, cedendo parte della sua sovranità, anche in riferimento al potere legislativo, nelle materie oggetto dei Trattati medesimi, con il solo limite dell'intangibilità dei principi e dei diritti fondamentali garantiti dalla Costituzione", sent 348/2007 cit.

Inoltre, la Corte – ed è questo in effetti a costituire il *proprium* dei giudizi sui conflitti[776] – dovrà anche valutare se l'esercizio in concreto di una data competenza, da parte dell'Autorità o viceversa di un altro potere dello Stato nei confronti dell'Autorità, possa o non meno modificare l'equilibrio fissatosi nell'assetto dei poteri in un dato momento storico.

A questo punto, viene in evidenza la questione se sono rinvenibili effettivamente potenziali margini di conflitto tra l'Autorità ed altri poteri dello Stato che non siano risolvibili con i mezzi ordinari del ricorso alla magistratura, proposto dal soggetto che si assume leso nelle proprie attribuzioni.

Data la trasversalità e la rilevanza delle funzioni esercitate dal Garante per la protezione dei dati personali, questo invero non può essere escluso a priori, richiedendo, appunto, una verifica in concreto del cd. tono costituzionale del conflitto.

Si pensi, ad esempio, ai casi in cui l'Autorità (ma anche altre Autorità indipendenti a cui si possa estendere il discorso) adotti atti non previsti esplicitamente dalla legge istitutiva, magari lesivi di attribuzioni del Parlamento o del Governo o del potere giudiziario. D'altra parte, il fatto che esistano funzioni non tipizzate delle Autorità indipendenti, dovute spesso alla formulazione del quadro normativo di riferimento, si è già evidenziato in precedenza .

Ancora più ampio è il ventaglio dei conflitti che potrebbero riguardare il cattivo uso del potere.

Il medesimo discorso, poi, può essere invertito, vedendo nell'Autorità il soggetto leso da atti o dal cattivo uso del potere da parte di altri poteri dello Stato, comprese, nel caso, altre Autorità.

Infine, alcune osservazioni in merito alla questione relativa a quale potere rappresenti il Garante per la protezione dei dati personali (o, nei termini indicati, le altre Autorità indipendenti), alla luce della tradizionale distinzione *organi –potere* e *poteri-organi*, nell'ambito dello Stato apparato a cui senz'altro appartiene[777].

[776] R. ROMBOLI, E. MALFATTI, S. PANIZZA, *Giustizia costituzionale*, Giappichelli, Torino, 2007.

[777] G.M. SALERNO, *I profili soggettivi nei conflitti di attribuzione relativi alla par condicio*, in F. MODUGNO (a cura di), *Par condicio e Costituzione*, Giuffrè, Milano, 1997, pag. 55.

Per il primo aspetto, si è parlato soprattutto di un potere esecutivo diffuso. Tale ricostruzione sarebbe in grado di salvare sia il carattere amministrativo dell'organo, sia la sua indipendenza, in special modo nei confronti del Governo.

Pertanto, con riferimento al Garante per la radio diffusione e l'editoria, oggetto delle pronunce costituzionali precedentemente indicate, si è detto che "il Garante, al pari di altri organismi consimili, può configurarsi come organo competente 'a dichiarare definitivamente la volontà del potere' a cui appartiene"[778]

Tuttavia, sarebbe alquanto contraddittorio sancire l'indipendenza delle Autorità e poi prevederne la rappresentanza in giudizio da parte del Governo, secondo la tradizionale interpretazione dell'art. 39 della l. n. 87/53, appare più opportuno allora attribuire la piena capacità processuale[779].

A tale ipotesi, è stata però obiettata la difficoltà di ritenere le Autorità (quindi anche il Garante per la protezione dei dati personali) riconducibili al potere esecutivo *stricto sensu*. Per le considerazioni illustrate in precedenza sulla loro attività, sarebbe meglio, quindi, ricostruire quali poteri-organi tali organismi (o meglio quelli cui sia effettivamente rinvenibile tale qualità), tenendo presente che il nostro ordinamento conosce già poteri situati fuori dall'area dei poteri tradizionali: vedi, ad esempio, la stessa Corte Costituzionale ed il Presidente della Repubblica, ai quali sarebbero quindi assimilabili le Autorità indipendenti, come espressione di poteri nuovi[780].

[778] Così G. GEMMA, *Garante per la radiodiffusione e l'editoria e conflitti di attribuzioni tra i poteri dello Stato*, in Giur. cost., 1995, pag. 1672.

[779] G. GEMMA, *Garante per la radiodiffusione e l'editoria e conflitti di attribuzioni tra i poteri dello Stato*, op. cit. 1673.

[780] E. CHELI, *Intervento*, in ISLE, Disciplina generale delle Autorità indipendenti, in Rass. Parl., 1999, pag 931, secondo il quale "le Autorità indipendenti, per la loro struttura e per la loro natura, non sono semplici articolazioni dei poteri amministrativi tradizionali, ma esprimono un potere nuovo". In questo senso anche G. Grosso, *Le Autorità amministrative indipendenti della Repubblica* , op. cit. pag. 280. Lo stesso riconosce la possibilità di qualificare "in primissima battuta"come poteri dello Stato l'Autorità antitrust, l'Autorità per le Garanzie nelle comunicazioni, il Garante della privacy, la CONSOB, la commissione per il diritto allo sciopero nei servizi pubblici essenziali, op. cit., pag 286; G.M. SALERNO, *I profili soggettivi nei conflitti di attribuzione relativi alla par condicio*, op. cit., pag 59.

5.2. I conflitti tra Stato e Regioni

Accanto ai conflitti tra poteri, va poi verificata la possibilità del sovrapporsi delle competenze fra le Autorità indipendenti e le Regioni, tale da poter essere oggetto di un ricorso per conflitto di fronte alla Corte Costituzionale.

In quest'ambito, come si vedrà, le modifiche sulla redistribuzione della competenze introdotte nel nuovo Titolo V della Costituzione hanno e avranno effettivamente un ruolo rilevante.

Al riguardo, prima della suddetta modifica normativa si segnala un ricorso proposto dalla Provincia autonoma di Trento, conclusosi con un'ordinanza della Corte costituzionale, l'ord. n. 378/2002[781]. Si trattava di un'ipotesi di interferenza fra le competenze della Provincia e quelle dell'Autorità di settore.

La Corte non ha deciso però nel merito, perché la Provincia ha raggiungo successivamente un'intesa con l'Autorità ed ha di conseguenza rinunciato al ricorso.

Quanto alla riforma del titolo V della Costituzione, in questo senso, questa accrescerà considerevolmente le possibili sovrapposizioni tra Autorità indipendenti ed altri soggetti istituzionali, con il rischio di possibili e reciproche invasioni di campo.

Per esempio, rispetto alle materie di legislazione concorrente (come l'ordinamento della comunicazione), che si intrecciano con attribuzioni di Autorità indipendenti, sarà necessario verificare in concreto che queste non si traducano "in un'ammissibile interferenza in procedimenti ormai facenti capo alla disciplina regionale"[782], fino al punto da poter rimettere in gioco la legittimità costituzionale delle leggi istitutive di alcune Autorità e, dall'altra parte, ipotizzare la possibilità di creazione di Autorità indipendenti regionali, prendendo magari ad esempio alcuni organismi già previsti da

[781] In Giur. Cost, 2002, pag, 2818 e ss, consultabile su http://www.giurcost.org/decisioni/index.html.

[782] Così P. DURET, *Autorità ed Agenzie e l'amministrazione in cammino*, in P. CAVALERI, G. DALLE VEDOVE, P. DURET (a cura di), Autorità indipendenti e Agenzie. Una ricerca giuridica interdisciplinare, Padova, Cedam, 2003, pag. 36.

alcuni statuti regionali oppure esperienze di altri ordinamenti, come la Spagna[783].

Anche sul versante della funzione amministrativa, il nuovo art. 118 Cost. pone evidenza, in una prospettiva diversa, il tipo di funzioni attribuite alle Autorità nei settori in cui queste intervengono.

Per quanto riguarda in particolare la competenza in materia di dati personali, si rileva l'intervento della Corte Costituzionale con la sentenza n. 271/05[784], emessa però in sede di ricorso diretto da parte del Presidente del Consiglio dei Ministri avverso legge della Regione Emilia-Romagna 24 maggio 2004, n. 11.

La suddetta pronuncia ha individuato nel D.lgs. n. 196/2003 "un corpo normativo essenzialmente riferibile, all'interno delle materie legislative di cui all'art. 117 Cost., alla categoria dell''ordinamento civile', di cui alla lettera l) del secondo comma (alla medesima disposizione ci si deve riferire per quanto attiene alle tutele giurisdizionali delle situazioni soggettive del settore, mentre le disposizioni relative al 'garante per la protezione dei dati personali' ed ai suoi poteri sono riconducibili alla lettera g del medesimo comma)"[785].

---

[783] Sul punto si rinvia a G. GRASSO, *Le Autorità amministrative indipendenti della Repubblica*, op cit., pag 180 e ss. In particolare, per quanto riguarda gli Statuti regionali si segnala come in alcuni di essi il difensore civico sia definito Autorità indipendente o Autorità di garanzia (es. art 72 statuto Liguri, art 90 statuto Piemonte, art. 50 statuto Puglia) oppure come lo Statuto ligure preveda un capo intitolato "Gli strumenti di garanzia", aperto dall'art 71, che stabilisce che " le Autorità indipendenti di garanzia istituite dal presente Statuto sono disciplinate da legge regionale", indicandole poi nel Difensore civico e nel Comitato regionale per le Comunicazioni.

Per l'esperienza spagnola, i due settori in cui operano congiuntamente Autorità nazionali e Autorità delle Comunità sono quello della protezione dei dati personali e quello della radiotelevisione. Quindi, accanto all'Agenzia de Proteccion de Datos, in Catalogna e nella Comunità autonoma di Madrid sono presenti due omologhe autorità autonomiste, mentre accanto all'Ente puplico RTVE sono presenti in quasi tutte le Comunità autonome corrispondenti Autorità, denominate Entes publicos de radioteleviosion.

[784] Consultabile su http://www.privacy.it/cortecost20050623.html. Si osserva che in merito al ricorso al Garante per la protezione dei dati personali è stato richiesto un parere dalla Presidenza del Consiglio dei Ministri, Dipartimento per gli affari regionali. I rilievi del Garante sono stati fatti propri dal Governo e il Consiglio dei ministri ha deciso di impugnare la legge davanti alla Corte Costituzionale (http://www.altalex.com/index.php?idnot=7636). Per quanto riguarda le leggi Regionali, è costante l'opera di monitoraggio da parte del Garante del rispetto della normativa statale, con segnalazione al Governo delle presunte violazioni. Si vedano le Relazioni annuali su www.garanteprivacy.it. Ancora si veda l'intervento di F.PIZZETTI, cit., in cui si sottolinea l'importanza di creare nuove forme di raccordo fra l'Autorità e gli Enti locali: "Siamo impegnati, in sostanza, su un grande spazio di attività (…) che ci mette sempre più al centro di una rete di rapporti fra Stato, regioni ed enti territoriali, che, a mio avviso, è una delle altre facce della costruzione di un sistema federale ben funzionante. Peraltro, dovremo anche noi stessi cercare nuove forme di interazione con le regioni e gli enti locali".

[785] Mentre alla Corte è apparso improprio, invece, "il riferimento alla competenza esclusiva dello Stato in tema di 'determinazione dei livelli essenziali delle prestazioni concernenti i diritti civili e sociali che devono essere garantiti su tutto il territorio nazionale', di cui alla lettera m) del secondo comma dell'art. 117 Cost., dal momento che la legislazione sui dati personali non concerne prestazioni, bensì la stessa

I giudici costituzionali hanno successivamente puntualizzato che, pur nell'ambito di questa esclusiva competenza Statale, residua anche una competenza legislativa dei soggetti pubblici che devono trattare dati personali, anche se "di tipo meramente integrativo", "evidentemente per la necessità, almeno in parte ineludibile, che i principi posti dalla legge a tutela dei dati personali siano garantiti nei diversi contesti legislativi ed istituzionali".

Quindi, possono essere adottati anche leggi o regolamenti regionali, "ma solo in quanto e nella misura in cui ciò sia appunto previsto dalla legislazione statale".

Precisa ulteriormente la Corte che "quanto appena espresso non equivale peraltro ad affermare la incompetenza del legislatore regionale a disciplinare procedure o strutture organizzative che prevedono il trattamento di dati personali, pur ovviamente nell'integrale rispetto della legislazione statale sulla loro protezione (ivi comprese le disposizioni relative alle 'misure minime di sicurezza' prescritte per i trattamenti dei dati personali con o senza l'utilizzazione degli strumenti elettronici)"[786].

In quest'ambito, secondo la Corte non è preclusiva nemmeno la titolarità esclusiva del legislatore statale in tema di "coordinamento informativo statistico e informatico dei dati dell'amministrazione statale, regionale e locale" (art 117, comma 2, lett. r).

Infatti, da una parte, il mancato intervento da parte dello Stato non preclude autonome iniziative della Regione – riconoscendo, tuttavia, che "il problema sorgerebbe solo nel momento in cui il legislatore statale dettasse normative nei medesimi ambiti a fine di coordinamento"- e dall'altra che "questo esclusivo potere legislativo statale concerne solo un coordinamento di tipo tecnico che venga ritenuto opportuno dal legislatore statale (si vedano le sentenze di questa Corte n. 31 del 2005 e n. 17 del 2004) e il cui

disciplina di una serie di diritti personali attribuiti ad ogni singolo interessato, consistenti nel potere di controllare le informazioni che lo riguardano e le modalità con cui viene effettuato il loro trattamento".

[786] "infatti le Regioni, nelle materie di propria competenza legislativa, non solo devono necessariamente prevedere l'utilizzazione di molteplici categorie di dati personali da parte di soggetti pubblici e privati, ma possono anche organizzare e disciplinare a livello regionale una rete informativa sulle realtà regionali, entro cui far confluire i diversi dati conoscitivi (personali e non personali) che sono nella disponibilità delle istituzioni regionali e locali o di altri soggetti interessati. Ciò, tuttavia, deve avvenire ovviamente nel rispetto degli eventuali livelli di riservatezza o di segreto, assoluti o relativi, che siano prescritti dalla legge statale in relazione ad alcune delle informazioni, nonché con i consensi necessari da parte delle diverse realtà istituzionali o sociali coinvolte".

esercizio, comunque, non può escludere una competenza regionale nella disciplina e gestione di una propria rete informativa (cfr. sentenza n. 50 del 2005)" .

Sono evidenti, pertanto, in materia di tutela di dati personali le potenziali sovrapposizioni di competenze o di sconfinamento reciproco fra Autorità nazionale e Regioni.

Questione diversa, invece, è accertare in concreto se le reciproche violazioni possano rimanere nell'ambito della giurisdizione del giudice ordinario (o amministrativo) e quando, al contrario, assumano il cd. tono costituzionale tale da giustificare l'intervento della Corte.

In quest'ultimo caso, la posizione eventuale delle Autorità è stata accosta a quella del potere giudiziario, nella consistente casistica di conflitti sollevati dalle Regioni nei confronti dei provvedimenti giurisdizionali, con la sistematica esclusione del giudice che ha emesso l'atto[787].

Infatti, se le Autorità indipendenti devono essere considerate appartenenti al potere esecutivo, sarebbe allora sostenibile una loro rappresentanza in giudizio da parte del Governo. Tuttavia, da quanto precedentemente osservato, l'indipendenza delle Autorità è un tratto ontologicamente distintivo delle stesse sia in termini organizzativi che funzionali, perciò si è evidenziato come sarebbe la stessa indipendenza "ad essere incompatibile con la disciplina dell'art 39, della l. n 87/53, così come lo era per il potere giudiziario"[788].

A maggior ragione le stesse considerazioni valgono se si qualificano le Autorità indipendenti come poteri autonomi.

In merito, poi, ai conflitti sollevati da Regioni nei confronti di atti giurisdizionali è stata evidenziata anche la possibilità di "un'interpretazione evolutiva dell'art 134 della Costituzione, ritenendo il conflitto Stato-

[787] G. GRASSO, *Le Autorità amministrative indipendenti della Repubblica*, op. cit., pag 289 e ss.; G. GRASSO, *Autorità amministrative indipendenti e conflitti intersoggettivi: una zona d'ombra della giustizia costituzionale?* , in Amministrazione in cammino, consultabile su http://www.amministrazioneincammino.luiss.it/wp-content/uploads/2010/03/Intervento.pdf; Sui conflitti intersoggettivi aventi ad oggetto atti giurisdizionali "i quali altro non sono, come orami universalmente accettato in dottrina, che dei veri e propri conflitti fra poteri neppure troppo mascherati", P. VERONESI, *Recenti tendenze in materia di conflitti di attribuzioni fra poteri. Profili soggettivi e oggettivi*, in Ann. Univ. Ferrara- Sc. Giur., Nuova serie, V. XVI (2002), consultabile su http://web.unife.it/progetti/annuali/scienze_giuridiche/2002/pdf/06.pdf; vedi anche R. PINARDI (a cura di) *Le zone d'ombra della giustizia costituzionale. I giudizi sui conflitti di attribuzione e sull'ammissibilità del referendum abrogativo*, Atti del seminario di Modena, 13 ottobre 2006, Giappichelli, Torino, 2007; P. BIANCHI, *Il conflitto di attribuzioni fra Stato e Regione e tra regioni*, in R. ROMBOLI (a cura di), Aggiornamenti in tema di processo costituzionale (2005-2007), Giappichelli, 2008.

[788] Così G. GRASSO, *Le Autorità amministrative indipendenti della Repubblica*, op. cit., pag 291.

Regione come riferito alla sola ipotesi in cui oggetto del conflitto sia un atto amministrativo, nella considerazione che esso è stato scritto in un momento in cui il conflitto fra lo Stato e le Regioni era visto come una *vindicatio potestatis* e quindi come conflitto fra l'esecutivo statale e quello regionale. Nel caso di atti giurisdizionali la Regione dovrebbe agire invece con lo strumento del conflitto fra poteri dello Stato"[789].

L'incremento delle ipotesi di conflitto su atti giurisdizionali promossi dalle Regioni così come la diversa collocazione che le stesse hanno assunto nell'ordinamento - vedi la citata riforma del titolo V della Costituzione - mettono straordinariamente in evidenza l'attualità dell'osservazione non solo in relazione al rapporto fra Regioni e potere giudiziario[790], ma anche nei confronti di atti di altri poteri dello Stato – fra cui quelli delle Autorità indipendente nei termini suddetti - con cui le competenze regionali possono oggi venire in contatto, richiamando, forse, la necessità di un aggiornamento della contrapposizione tra conflitti fra enti e tra conflitti tra poteri[791].

[789] Così R. ROMBOLI, *Storia di un conflitto partito tra enti ed arrivato tra poteri. (Il conflitto tra lo Stato e la Regione avente ad oggetto un atto giurisdizionale)*, in La Corte costituzionale e gli altri poteri dello Stato, a cura di A_ ANZON, B. CATAVITA, M. LUCIANI e M. VOLPI, Giappichelli, Torino, 1993, pag. 203 e ss.

[790]Nella sent. n. 309/2000 la Corte ha sostenuto, tuttavia, che si può porre rimedio alla carenza nella rappresentanza in giudizio del giudice soltanto "in via normativa, non essendo possibile ovviare a essa in via di interpretazione e applicazione dell'ordinamento vigente", per la mancanza di "indicazioni sufficienti circa il modo di colmare la lacuna". Nel giugno del 2004 la stessa ha modificato le Norme Integrative, inserendo all'art. 27 un secondo comma, che stabilisce che, in caso di conflitto intersoggettivo, il ricorso debba "essere notificato altresì all'organo che ha emanato l'atto, quando si tratti di autorità diverse da quelle di Governo e da quelle dipendenti dal Governo". Nell'ord. n. 353/2006, i Giudici costituzionali hanno applicato per la prima volta questa nuova disposizione, che sebbene non risolutiva, "significa evidentemente riconoscere l'esistenza di conflitti relativi a sfere di competenze dello Stato, che non si possono ricondurre all'indirizzo politico amministrativo dell'art. 95 Cost., come quelle dei giudici, della Corte dei conti, delle Autorità amministrative indipendenti." - così G. GRASSO, *Autorità amministrative indipendenti e conflitti intersoggettivi: una zona d'ombra della giustizia costituzionale?*, op. cit.. Tuttavia, questo non può integrare un contraddittorio necessario a favore del giudice. Sul punto vedi anche T. GIOVANNETTI, *I «soggetti esclusi» nei conflitti di attribuzione*, in R. PINARDI (a cura di) *Le zone d'ombra della giustizia costituzionale. I giudizi sui conflitti di attribuzione e sull'ammissibilità del referendum abrogativo*, op. cit., il quale ipotizza che "il magistrato potrebbe provare la strada dell'intervento in giudizio, ai sensi del combinato disposto degli art. 27, comma 2, e 4 delle N.I. (il quale ultimo ... parla genericamente di 'altri soggetti', senza distinzione tra soggetti pubblici e privati, tra terzi o organi dello Stato), almeno nelle ipotesi in cui il Presidente del Consiglio scegliesse di non costituirsi", ma poi si chiede "se risulti legittimo, oltre che appagante, risolvere una questione che attiene, di fatto, al piano della legittimazione ad essere "parte" del conflitto, operando sul piano dell'intervento nel contraddittorio".

[791] In questi termini vedi G. Grasso "Che obiettivo dei conflitti costituzionali sia conformare o meno soggetti, organi e istituzioni al principio della massima inclusione possibile, la via maestra per illuminare davvero le zone d'ombra della giustizia costituzionale sui conflitti(…) è riconoscere ai diversi organi in esame (giudici ed Autorità amministrative indipendenti, le seconde però non in modo generalizzato, ma caso a caso) la possibilità di ricorrere e di resistere autonomamente in giudizio. (…)il conflitto intersoggettivo, a tali condizioni, modificherebbe le sue caratteristiche essenziali, subendo un'inevitabile torsione, così da trasformarsi in un conflitto misto e spurio, a metà tra i due modelli di conflitto espressamente indicati in Costituzione", in *Autorità amministrative indipendenti e conflitti intersoggettivi: una zona d'ombra della giustizia costituzionale?*, op. cit.. e più diffusamente in *Il conflitto di attribuzioni tra le Regioni e il potere giudiziario*, Giuffrè, Milano, 2001, 228 ss.

5.3. Il Garante per la protezione dei dati personali come giudice *a quo* nel giudizio costituzionale incidentale

La partecipazione delle Autorità indipendenti e nello specifico del Garante per la protezione dei dati personali ai conflitti costituzionali non esaurisce le ipotesi di rapporto fra queste e la giustizia costituzionale.

Ci si riferisce, in particolare, alla possibilità di attribuire ad alcune di queste Autorità, fra cui il Garante della privacy, la natura di giudici *a quibus* e di conseguenza il potere di sollevare questione di legittimità costituzionale davanti alla Corte Costituzionale.

La configurabilità di tale ipotesi è stata suggerita dalla constatazione che alcune volte la Corte ha avallato una nozione ampia di "giurisdizione", tanto da estendere la nozione di giudice *a quo* sino a ricomprendere organi che non sembrano potersi ritenere giurisdizionali, ma che sono stati ritenuti tali "ai limitati fini" della proposizione della questione di costituzionalità.

L'analisi, pertanto, è senza dubbio delicata, in quanto alla difficoltà di individuare i confini certi della nozione di "giudice" e di "giudizio", anche alla luce della giurisprudenza della Corte costituzionale, si intrecciano le questioni legate alle figure delle Autorità indipendenti che, come si è visto, sono fra le più controverse, quanto a natura giuridica, organizzazione interna, funzionamento e collocazione nell'ordinamento costituzionale.

Per quanto riguarda il primo aspetto, la natura del giudizio incidentale, connessa al legame necessario tra il giudizio sulla legge e quello da cui ha tratto origine il dubbio di costituzionalità con l'interesse oggettivo all'eliminazione dall'ordinamento delle leggi incostituzionali,[792] non ha permesso di avere criteri univoci nell'individuazione dei soggetti legittimati a sollevare la questione di legittimità costituzionale.

Operazione quest'ultima particolarmente sensibile anche perché "va a modificare, seppur in veste di una tessera del mosaico, l'intero sistema di

[792] In altre parole, "la sua perpetua oscillazione fra polo della concretezza (giustizia del caso singolo e tutela dei diritti-interessi legittimi dei consociati) e polo dell'astrattezza (tutela dei valori obiettivi e generali dell'ordinamento costituzionale)". Così A. CERRI, *Corso di giustizia costituzionale*, II ed., Giuffrè, Milano, 1997, pag. 51.

giustizia costituzionale, sempre in movimento, il quale condiziona a sua volta, la singola tessera"[793].

Così, nei primi anni di attività la Corte ha seguito un'interpretazione lata dei concetti di "giudice" e di "giudizio"[794], a cui ha fatto seguito, invece, un atteggiamento restrittivo che ha portato ad autorizzare l'introduzione di un giudizio incidentale sulle leggi solo per il giudice che, oltre ad essere inserito stabilmente nell'ordine giudiziario, operasse all'interno di un giudizio: ovvero, nell'ambito di un procedimento avente carattere giurisdizionale ed in cui la soluzione dell'eccezione fosse pregiudiziale per l'emanazione di un provvedimento giurisdizionale[795].

Tuttavia, non sono mancate pronunce in cui la Corte ha accolto una nozione "funzionale" e "sostanziale" di "giudice" e di giudizio".

Questo si è verificato, ad esempio, con la sentenza n. 226/1976[796], in cui la Corte dei conti è stata riconosciuta quale giudice *a quo* in sede di controllo preventivo, in quanto anche "se il procedimento svolgentesi davanti alla Sezione di controllo non é un giudizio in senso tecnico-processuale, é certo tuttavia che, *ai limitati fini* [corsivo dello scrivente]

[793] F. CECAMORE, *L'autorità indipendente come giudice a quo nel giudizio costituzionale*, in R. BALDUZZI, P. COSTANZO (a cura di), Le zone d'ombra della giustizia costituzionale. I giudizi sulle leggi, op. cit., pag 115.

[794] Vedi ad esempio la sentenza 83 del 1976, redattore Costantino Mortati, in cui si afferma che: "La Corte, nelle sue precedenti pronunce, ha ritenuto che gli artt. 1 della legge costituzionale n. 1 del 1948, 23 della legge n. 87 del 1953 e 1 delle Norme integrative consentano una determinazione dei requisiti necessari alla valida proposizione delle questioni stesse, tale da condurre, per una parte, a far considerare 'autorità giurisdizionale' anche organi che, pur estranei all'organizzazione della giurisdizione ed istituzionalmente adibiti a compiti di diversa natura, siano tuttavia investiti, anche in via eccezionale, di funzioni giudicanti per l'obiettiva applicazione della legge, ed all'uopo posti in posizione *super partes*, e per un'altra a conferire carattere di 'giudizio' a procedimenti che, quale che sia la loro natura e le modalità di svolgimento, si compiano però alla presenza e sotto la direzione del titolare di un ufficio giurisdizionale."

[795] Cfr. R. ROMBOLI, E. MALFATTI, S. PANIZZA, *Giustizia costituzionale*, op. cit.

[796] Consultabile su http://www.giurcost.org/decisioni/1976/0226s-76.html: "le sentenze nn. 165 del 1963, 121 del 1966, 142 e 143 del 1968 ne hanno affermato la legittimazione a sollevare questioni di costituzionalità nel corso del giudizio di parificazione (così dei rendiconti regionali come del rendiconto generale dello Stato) pur essendo detto giudizio regolato dal T.U. 12 luglio 1934, n. 1214, nel cap. IV, e non già nel capitolo successivo, che é quello concernente le 'attribuzioni giurisdizionali' della Corte, e in ordine ad esso l'art. 40 del medesimo testo unico limitandosi a richiamare 'le formalità della sua giurisdizione contenziosa': con l'avvertenza, peraltro, che, in questa sede, la Corte dei conti 'non applica le leggi sostanziali di spesa riflettentisi nei capitoli del bilancio, e neppure applica la legge di approvazione del bilancio, avendole 'già applicate in corso di esercizio, operando il riscontro di legittimità sui singoli atti soggetti al suo controllo (…).

3. - Ed infatti, procedendo al controllo sugli atti del Governo, la Corte dei conti applica le norme di legge da cui questi sono disciplinati, ammettendoli al visto e registrazione, soltanto se ad esse conformi: di tal che, essendo strettamente vincolata dalle leggi in vigore, potrebb'essere costretta, in pratica, a rifiutare il visto quando l'atto contrasti con norme pur di dubbia costituzionalità, o viceversa ad apporlo anche ove sia stato adottato sulla base e nel rispetto di norme, che siano, a loro volta, di dubbia costituzionalità. Nell'una e nell'altra ipotesi, la situazione é, dunque, analoga a quella in cui si trova un qualsiasi giudice (ordinario o speciale), allorché procede a raffrontare i fatti e gli atti dei quali deve giudicare alle leggi che li concernono".

dell'art. 1 della legge cost. n. 1 del 1948 e dell'art. 23 della legge n. 87 del 1953, la funzione in quella sede svolta dalla Corte dei conti é, sotto molteplici aspetti, analoga alla funzione giurisdizionale, piuttosto che assimilabile a quella amministrativa, risolvendosi nel valutare la conformità degli atti che ne formano oggetto alle norme del diritto oggettivo, ad esclusione di qualsiasi apprezzamento che non sia di ordine strettamente giuridico. Il controllo effettuato dalla Corte dei conti é un controllo esterno, rigorosamente neutrale e disinteressato, volto unicamente a garantire la legalità degli atti ad essa sottoposti, e cioè preordinato a tutela del diritto oggettivo, che si differenzia pertanto nettamente dai controlli c.d. amministrativi, svolgentisi nell'interno della pubblica Amministrazione; ed é altresì diverso anche da altri controlli, che pur presentano le caratteristiche da ultimo rilevate, in ragione della natura e della posizione dell'organo cui é affidato".

"(..)D'altronde, sul piano sostanziale, il riconoscimento di tale legittimazione si giustifica anche con l'esigenza di ammettere al sindacato della Corte costituzionale leggi che, come nella fattispecie in esame, più difficilmente verrebbero, per altra via, ad essa sottoposte".

Più recentemente la stessa apertura è avvenuta, come noto, in merito alla legittimazione a sollevare questione di legittimità costituzionale da parte degli arbitri, nell'arbitrato rituale, con la sentenza n. 376/2001[797].

La Corte ha ragionato, secondo la tecnica dei "limitati fini" della proponibilità della questione di costituzionalità, sulla natura dell'arbitro e della sua attività per consentire al collegio arbitrale una via di accesso[798], rilevando in sintesi che "in un assetto costituzionale nel quale è precluso ad ogni organo giudicante tanto il potere di disapplicare le leggi, quanto quello

[797] Consultabile su http://www.giurcost.org/decisioni/2001/0376s-01.html.

[798] Via che si potrebbe avere però in sede di impugnazione del lodo. La richiesta nella giurisprudenza costituzionale del carattere "della definitività del provvedimento emanato dal soggetto pur esterno all'ordine giudiziario" "sembrerebbe escludere le accennate evenienze di rimessione [arbitri e autorità amministrative indipendenti], perché in entrambi i casi ipotizzati, essendo previste dall'ordinamento apposite sedi per l'impugnazione degli atti di competenza di quei soggetti è configurabile l'eventuale successivo giudizio" nel quale fare emergere la questione di costituzionalità. Così si osservava prima della sentenza sui collegi arbitrali, P. BIANCHI, E. MALFATTI, *L'accesso in via incidentale*, in A. ANZON, P. CARETTI, S. GRASSI (a cura di) Prospettive di accesso alla giustizia costituzionale, Giappichelli, Torino, 2000, pag. 24.

di definire il giudizio applicando leggi di dubbia costituzionalità, anche gli arbitri debbono utilizzare il sistema di sindacato incidentale sulle leggi"[799].

Tale soluzione ha trovato in seguito un'implicita conferma nell'ord. n. 11/2003[800], oggi peraltro espressamente recepita a livello normativo dall'articolo 22 del D.lgs. n. 40/2006 (art 819 bis c.p.c.), che ha previsto la "sospensione del *procedimento* arbitrale" quando gli arbitri "rimettono alla Corte costituzionale una questione di legittimità costituzionale".

L'apertura del giudizio incidentale ad un soggetto comunque privato, qual è il collegio arbitrale, dovrebbe, quindi, sollecitare altri soggetti a tentare di essere a loro volta legittimati[801]. Tuttavia, allo stato questo non è avvenuto però per le Autorità indipendenti, che, invece, hanno continuato ad evitare di ricorrere alla Corte[802], mentre ha avuto esito negativo, ad esempio, nei confronti del Consiglio di Stato, in sede consultiva nell'ambito del ricorso straordinario al Capo dello Stato, con la sentenza n. 254/2004[803], confermata con le ordinanze nn. 357 e 392/2004.

Al riguardo, è indubbia la presenza nel suddetto ricorso straordinario al Presidente della Repubblica di una serie di elementi sia di giurisdizionalità sia di altri, invece, di natura amministrativa.

La Corte costituzionale con la sentenza citata ne ha rinvenuto, infine, la natura amministrativa, citando specificatamente l'art. 14, comma 1, D.P.R.. n. 1199/1971, in base al quale, ove il Ministro competente intenda proporre al Capo dello Stato una decisione difforme dal parere del Consiglio di Stato,

---

[799] "Il riconoscimento della legittimazione degli arbitri potrebbe comportare un ben maggiore ampliamento dell'accesso alla Corte costituzionale, rispetto a quello che può apparire *prima facie* essendo chiaramente facilitato il ricorso a *lites fictae* create allo scopo di sottoporre alla Corte un dubbio di legittimità costituzionale e potendo, entro certi limiti tradursi in una sorta di ricorso diretto alla giustizia costituzionale" Così R. ROMBOLI, E. MALFATTI, S. PANIZZA, *Giustizia costituzionale*, op. cit.

[800] Consultabile su http://www.giurcost.org/decisioni/2003/0011o-03.html.

[801] M. ESPOSITO, *Si aprono le «porte del cielo»: dall'arbitrato al ricorso straordinario al Presidente della Repubblica?*, in Giur. Cost., 2001, 3768 e ss.; R. PINARDI, *Quando l'arbitro diventa portiere (della Corte): notazioni minime sulla "naturale" elasticità della nozione di giudice a quo*, in Giur. Cost., 2001, 3756.; E. FURNO, *Corte costituzionale e arbitrati: un nuovo "giudice a quo"?*, in Giur. it., 2004, pag. 437.

[802] Peraltro la rilevata prudenza delle Autorità indipendenti è stata ritenuta giustificata se messa a confronto con la diversa vicenda che ha riguardato, come si vedrà, il Consiglio di Stato, in sede di ricorso straordinario al Presidente della Repubblica. Così A. P. GRIFFI, *Accesso incidentale alla Corte costituzionale e tutela dei diritti: note minime anche a proposito delle Authorities*, Intervento al convegno, organizzato da APro.M, dalle varie Associazioni nazionali dei magistrati, sia ordinari sia amministrativi, dal C.N.F. e dalla F.N.S.I. su Politica, Economia e Giustizia. La tutela dei diritti e delle libertà dei cittadini come fattori di garanzia, Tar Lazio, Sala Conferenze, 1 marzo 2006, consultabile su http://www.giustizia-amministrativa.it/documentazione/studi_contributi/Patroni_Griffi_Accesso_incidentalealla CC.htm#_ftnref11.

[803] Per un commento della sentenza in senso critico, vedi A. P. GRIFFI, *Accesso incidentale alla Corte costituzionale e tutela dei diritti: note minime anche a proposito delle Authorities*, op cit.

deve sottoporre la questione al Consiglio dei Ministri, il cui provvedimento, riconosce la Corte non può essere ritenuto di carattere giurisdizionale.

Tuttavia, deve essere messo in evidenza che legge n. 69/2009, recante "Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile", è a sua volta intervenuta sul punto, modificando gli artt. 13 e 14 del D.P.R.. 1199/1971.

In particolare, il legislatore ha inciso sulla funzione e sul peso del parere, oggi vincolante, del Consiglio di Stato in seno al procedimento, spostando decisamente l'istituito verso la natura giurisdizionale, piuttosto che amministrativa, e soprattutto ha previsto espressamente la legittimazione del Consiglio di Stato a sollevare questione di legittimità costituzionale nella relativa sede consultiva[804].

In relazione all'oggetto della presente analisi, viene da chiedersi se l'iniziativa presa dal legislatore con il Consiglio di Stato, ovvero di "baipassare" in questo modo la riserva di legge costituzionale, prevista dall'art. 137, comma 1 della Costituzione, e la specificazione in concreto dei requisiti di "giudice" e di "giudizio" rimessa alla Corte costituzionale, possa aprire le porte ad analoghi interventi a favore di altri organismi.

Come si è visto, infatti, la natura delle Autorità indipendenti è tutt'altro che pacifica e, nello specifico, non lo è quella del Garante per la protezione dei dati personali.

Nonostante, infatti, la Corte di Cassazione abbia ricondotto i poteri decisori dell'Autorità nell'ambito dell'amministrazione[805], una posizione differente è manifestata, da chi non condivide la riconducibilità di tutte le funzioni esercitate *sic e simpliciter* all'attività amministrativa.

Al Garante, oltre alla cognizione dei diritti sul trattamento dei dati personali, è attribuito in realtà un rilevante potere decisorio d'urgenza di natura cautelare, avendo, come illustrato, la facoltà di ordinare il blocco immediato del trattamento dei dati, nonché il potere di disporre le modalità

[804] Sulla legittimità costituzionale ti tale intervento, si rinvia a N. PIGNATELLI, *Sulla natura del ricorso straordinario: l'illegittimità costituzionale dell'art. 69 della l. 69/2009*, consultabile su http://www.forumcostituzionale.it/site/images/stories/pdf/documenti_forum/temi_attualita/presidente_repubblica/0003_pignatelli.pdf e dello stesso autore, *Sulla " natura" del ricorso straordinario: la scelta del legislatore (art. 69 l. 69/2009)*, in Rivista Neldiritto, Speciale. Le nuove norme su procedimento e processo amministrativo. Commento alle novità introdotte dalla legge 18 giugno 2009, n. 69, consultabile su http://www.giustizia-amministrativa.it/documentazione/studi_contributi/2009_7_Pignatelli_Le_scelte_del_legislatore.htm.

[805] Cass civ, sez. I, 20 maggio 2002, n. 7341, cit, confermata successivamente dalla sentenza, Cass, civ. sez. I, 25 giugno 2004, n. 11864.

di attuazione dei provvedimenti adottati, "avvalendosi se necessario del personale dell'ufficio o della collaborazione di altri organi dello Stato"[806].

Ancora, lo stesso adotta provvedimenti in alternativa alla tutela giurisdizionale, per cui è previsto anche un termine di impugnazione davanti al Tribunale, con la possibilità, quindi, che questi diventino definitivi, pur se non suscettibili di assumere la natura di giudicato.

E' prevista, inoltre, una fattispecie autonoma di reato, consistente nell'inosservanza dei provvedimenti del Garante[807].

Si poi già evidenziata la forma giudiziaria che permea parte dell'attività del Garante: l'audizione delle parti, l'obbligo di motivazione, i poteri strumentali di indagine e di ispezione, ecc.[808]

Per di più, la titolarità di poteri decisori per la risoluzione di controversie si combina ulteriormente con l'indipendenza dell'Autorità, facendo assumere alla stessa un ruolo comunque *super partes*, anche se diverso dalla terzietà del giudice, per i motivi che si sono già sottolineati.

Pertanto, nella "confusione"[809] che coinvolge la natura del Garante e delle Autorità indipendenti in generale, sarebbe effettivamente molto utile un intervento chiarificatore della Corte costituzionale.

Una decisione di una certa rilevanza su questo tema, peraltro, è rintracciabile nella sentenza n. 57 del 1995[810], in cui la Corte ha attribuito alla Commissione di garanzia dello sciopero nei servizi pubblici essenziali la qualificazione di soggetto appunto *super partes* ad alta competenza, rivenendo nella sua attività il principio del contraddittorio.

Questo è stato visto da qualcuno come un velato – ma invero molto velato - sbilanciamento della Corte a favore di un impostazione non amministrativa in senso stretto e tradizionale di questa Autorità[811].

Significativa è apparsa anche un'altra decisione, la sentenza n. 482 del 1995[812], con cui è stato riconosciuto che con l'Autorità di vigilanza sui

[806] Art 150, comma 5, D.lgs. n. 196/2003.

[807] Art. 170, D.lgs. n. 196/2003.

[808] F. CECAMORE, *L'autorità indipendente come giudice a quo nel giudizio costituzionale*, in op. cit. pag 130

[809] Idem.

[810] Consultabile su http://www.giurcost.org/decisioni/1995/0057S-95.htm

[811] Così G. GRASSO, *La Corte costituzionale si pronuncia solo parzialmente sulla natura giuridica e sulla collocazione costituzionale delle Autorità indipendenti. Considerazioni sparse sulle decisioni n. 57, n. 118 e n. 226 del 1995*, in Quad. Reg., 1995, pag. 246.

[812] Consultabile su http://www.giurcost.org/decisioni/1995/0482s-95.htm.

lavori pubblici è stato costituito "secondo linee che si affermano anche in altri settori nei quali si è manifestata l'esigenza di avere un'autorità indipendente, un nuovo organismo collegiale di alta qualificazione, chiamato ad operare in piena autonomia rispetto agli apparati dell'esecutivo ed agli organi di ogni amministrazione.".

Inoltre, è stata esclusa una totale assimilazione di tale Autorità ad un organo amministrativo: secondo la Corte, intatti, "le attribuzioni dell'Autorità non sostituiscono né surrogano alcuna competenza di amministrazione attiva o di controllo; esse esprimono una funzione di garanzia, in ragione della quale è configurata l'indipendenza dell'organo. Le attività rimesse all'Autorità assumono carattere strumentale rispetto alla conoscenza ed alla vigilanza nel complessivo settore dei lavori pubblici". Inoltre, la Corte ha tenuto presente che Autorità gode di un particolare rapporto con il Parlamento, derivante dal sistema di nomina dei suoi cinque membri e dalla relazione annuale che l'Autorità è tenuta a trasmettere.

Sebbene le osservazioni della Corte costituzionale si prestino ad essere trasposte ad altre Autorità, in specie al Garante per la protezione dei dati personali, tuttavia oltre le suddette valutazioni la sentenza non è andata.

Sempre in merito alla qualificazione delle Autorità come giudici *a quibus* deve riconoscersi che in caso negativo non mancherebbe la possibilità di sottoporre, comunque, alla Corte costituzionale leggi che si ritengano viziate di incostituzionalità.

Le decisioni delle Autorità sono, infatti, tutte impugnabili davanti all'autorità giudiziaria (amministrativa o ordinaria) ed in quest'ambito sarebbe sicuramente possibile sollevare questione di costituzionalità.

Tuttavia, si è osservato che escludere, ad esempio, il Garante della privacy dalla legittimazione a sollevare questione di costituzionalità significherebbe che nel caso lo stesso ravvisasse - o fosse eccepita dalle parti - l'illegittimità costituzionale di una disposizione procedurale, questo sarebbe comunque tenuto ad applicare la norma, pur in presenza di una questione rilevante e non manifestamente infondata[813]. Risollevare, difatti, la questione davanti al giudice ordinario, in sede di opposizione al

[813] A meno che non si ritenga che in questo caso il Garante non debba adottare alcun provvedimento, configurando così un'ipotesi di silenzio- rifiuto, prevista dal D.lgs. n. 196/2003, artt. 150, comma 2 e 151.

provvedimento del Garante, richiederebbe di doverne verificare anche la rilevanza, che in quella sede sembra in realtà mancare.

"Così, senza un canale di accesso alla giustizia costituzionale, l'Autorità, il cui compito è di garantire specifici diritti costituzionalmente garantiti, si troverebbe ad applicare una legge, pur ritenendola incostituzionale"[814].

La Corte costituzionale, quindi, potrebbe far uso degli argomenti già utilizzati per verificare caso per caso l'attività svolta dalle singole Autorità e assimilarla alla nozione di "giudice" e di "giudizio" ai "limitati fini" della legittimazione a sollevare questione di legittimità costituzionale.

Questo non tanto per far in modo che alcune leggi si sottraggano al sindacato di costituzionalità, in quanto come si è visto, si tratterebbe semmai solo delle norme procedurali, quanto piuttosto evitare comunque la produzione di effetti lesivi di diritti costituzionalmente rilevanti, derivante dall'emissione di provvedimenti immediatamente esecutivi, adottati sulla base di norme incostituzionali.

Qui evidentemente il "pendolo" relativo alla natura del giudizio costituzionale incidentale sarebbe sbilanciato verso "polo della concretezza", anche se forse in maniera non dissimile da quanto è stato già riconosciuto per gli arbitri.

Senza dubbio un'eventuale ammissibilità della possibilità di proporre questione incidentale, potrebbe mettere in discussione la possibilità, oggi indubbia, di partecipazione del Garante per la protezione dei dati personali nei giudizio davanti al giudice ordinario sia in sede di ricorso diretto sia in sede di opposizione ai provvedimenti dell'Autorità, per far valere "lo stesso interesse pubblico in funzione del quale esso è predisposto"[815].

In tal caso, allora, sarebbe da chiedersi se sia più utile, in termini di tutela dei diritti degli interessati o di tutela oggettiva della legittimità costituzionale della normativa di settore, la presenza del Garante in sede giurisdizionale oppure la qualifica di *giudice a quo* nel procedimento giustiziale davanti a se medesimo.

Altro argomento ancora è il timore dell'eccessivo aumento delle pendenze, che potrebbe derivare dall'apertura nei confronti di alcune

[814] Così F. CECAMORE, *L'autorità indipendente come giudice a quo nel giudizio costituzionale*, in op. cit. pag 140.

[815] Sent. C. Cass., Sez. I civile, 20 maggio 2002, n. 7341, cit.

Autorità indipendenti, paventato come motivo che potrebbe indurre di fatto la Corte ad affrontare la questione con particolare prudenza e rigore[816].

L'opinione negativa in ordine alla configurabilità delle Autorità indipendenti come giudici *a quibus*, si fonda, in ultima analisi, sulla considerazione generale del loro ruolo, il quale presenta un cumulo di funzioni normative, provvedimentali, giustiziali tali da porle in una "posizione sostanzialmente diversa rispetto a qualsiasi autorità soggettivamente o oggettivamente giurisdizionale, che di simili competenze non dispone affatto"[817].

In tal senso viene anche evidenziata "la posizione privilegiata di dialogo con il legislatore e gli organi politici complessivamente intesi, grazie alle funzioni di suggerimento, di stimolo, di sollecitazione a rimuovere o modificare gli atti normativi che ostacolano la realizzazione dei diritti garantiti"[818].

In ogni caso, preso atto del fatto che le Autorità indipendenti costituiscono per molti profili dei punti di riferimento sulla materie a loro affidate e sui diritti a tali settori connessi e che, per i profili analizzati, i loro poteri decisori sono strutturati in maniera "simile" ai procedimenti giurisdizionali (tanto da parlare di para-giurisdizionalità), la loro valutazione, in positivo o negativo, come eventuali "portieri" del giudizio costituzionale incidentale meriterebbe di non essere trascurata. Certo è, però, che le prime a dover prendere l'iniziativa in tal senso dovrebbero essere proprio le Autorità indipendenti, trovando il coraggio di bussare alla porta della Corte costituzionale.

6. Il ricorso pregiudiziale alla Corte di giustizia

E' stato messo più volte in evidenza in questa sede il legame particolarmente forte fra il Garante per la protezione dei dati personali e la normativa europea.

816 Vedi F. CECAMORE, *L'autorità indipendente come giudice a quo nel giudizio costituzionale*, in op. cit. pag 142.

817 M. MANETTI, *Profili di giustizia costituzionale delle autorità indipendenti*, op. cit., pag. 41.

818 M. MANETTI, ult, op. cit., pag. 41. La stessa qualifica tale attività come una vera e propria "funzione *latu sensu* di iniziativa di iniziativa legislativa".

In particolare, si è evidenziato come a seguito dell'entrata in vigore del Trattato di Lisbona, sia il Trattato sull'Unione europea, sia il Trattato sul funzionamento dell'Unione, sia la Carta dei diritti fondamentali dell'Unione, prevedano espressamente la figura di un'Autorità indipendente, con funzione di controllo dell'applicazione della normativa comunitaria in materia di tutela dei dati personali.

Come noto, il principio della preminenza del diritto comunitario impone non solo al giudice, ma allo Stato nel suo insieme, dunque a tutte le sue articolazioni, ivi comprese le amministrazioni, di dare piena efficacia alla norma comunitaria e, in caso di conflitto di una norma nazionale con una norma comunitaria provvista di effetto diretto, di disapplicare quella dello Stato[819].

Si deve ritenere, quindi, che anche in caso di contrasto il Garante debba applicare la normativa comunitaria, disapplicando quella interna.

Data poi la materia, la cui disciplina si è visto avere sotto molti aspetti rilevanza sovranazionale, è poi estremamente probabile che anche nella sede del procedimento contenzioso di cui si è trattato il Garante si possa trovare nella condizione di dover valutare se la normativa nazionale si ponga o meno in contrasto con quella comunitaria, così come è verosimile che nello stesso procedimento possa altresì sorgere un dubbio sull'interpretazione di una norma comunitaria.

Orbene, le riflessioni precedentemente fatte in ordine al natura dell'attività decisoria del Garante per la protezione dei dati personali, portano a fare qui qualche considerazione anche sull'eventuale possibilità che, in questo caso la Corte di giustizia, possa ritenere il Garante – ma nel caso anche altre Autorità indipendenti – legittimato a sollevare questione pregiudiziale ai sensi dell'art. 267 TFUE (ex articolo 234 del TCE)[820].

Al riguardo, è pacifico che il sistema del rinvio pregiudiziale costituisca un meccanismo fondamentale del diritto dell'Unione europea, avente per

[819] Fra le numerose si veda Sent. 9 marzo 1978, causa 106/77, Simmenthal, in *Racc. Giur. Corte Giust.*, 1978, 629 ss., specie par. 24; CGCE, 28 giugno 2001, C-118/00, *Larsy*, punto 52.; CGCE, 9 settembre 2003, C-198/01, *Consorzio Industrie Fiammiferi*, punto 49. Cfr anche sull'argomento A. CELOTTO, *La prevalenza del Diritto comunitario sul Diritto degli Stati: ambito e portata della disapplicazione*, in http://www.iidpc.org/revistas/8/pdf/129_145.pdf.

[820] Per la dottrina in tal senso vedi F.P. LUISO, sub *Art. 29*, in C.M. BIANCA, F.D. BUSNELLI, (a cura di), Tutela della privacy, op. cit., pag 674 (con riferimento all'allora art. 177, comma 3, del Trattato). Contra M. MANETTI, *Profili di giustizia costituzionale delle autorità indipendenti*, op. cit. pag 40.

scopo quello di fornire ai giudici nazionali lo strumento per assicurare un'interpretazione e un'applicazione uniformi di tale diritto, in tutti gli Stati membri.

La Corte di giustizia dell'Unione europea è il soggetto competente a pronunciarsi in via pregiudiziale sull'interpretazione del diritto dell'Unione europea e sulla validità degli atti adottati dalle istituzioni, dagli organi e organismi dell'Unione, a seguito di domanda sollevata "da un organo giurisdizionale di uno degli Stati membri"[821].

Definire cosa s'intenda per organo giurisdizionale nazionale è "questione unicamente di diritto comunitario" ed in particolare della Corte di giustizia, le cui valutazioni, pertanto, sono autonome e possono non coincidere con quelle relative all'organo, operate nell'ordinamento nazionale.

Così è stato, ad esempio, per quanto riguarda il Consiglio di Stato in sede di ricorso straordinario al Capo dello Stato. Mentre la Corte costituzionale, si è visto, non ha rinvenuto nel procedimento i requisiti necessari per l'individuazione di un "giudizio" e di "giudice", ai fini della legittimazione a sollevare questione incidentale di costituzionalità[822], la Corte di giustizia ha ritenuto invece il Consiglio di Stato, nella suddetta sede, organo legittimato a sollevare la cd. pregiudiziale comunitaria[823].

Quindi, anche un'eventuale pronuncia da parte della Corte costituzionale riguardo le questioni, precedentemente accennate, relative al Garante per la protezione dei dati personali - così come in generale alle altre Autorità indipendenti ad esso assimilabili -potrebbe non coincidere necessariamente

821 Cfr. Nota informativa della Corte di Giustizia 2009/C 297/01, riguardante le domande di pronuncia pregiudiziale da parte dei giudici nazionali, Gazzetta Ufficiale dell'UE serie C 297 del 5.12.2009, consultabile su http://www.altalex.com/index.php?idnot=48436.

822 Sent. 256/2004, cit., ma vedi anche Sent. Cass. Sez. Un. 18 dicembre 2001, n. 15978, consultabile su http://www.altalex.com/index.php?idnot=4550, la quale nega la natura giurisdizionale del decreto con il quale è deciso il ricorso straordinario al Capo dello Stato, in cui i si legge: "Invero, la nozione di 'organo giurisdizionale' rilevante ai fini della individuazione delle autorità legittimate a rimettere 'in via pregiudiziale' all'esame della Corte di Giustizia questioni relative all'interpretazione del Trattato e all'interpretazione e alla validità degli atti compiuti dalle istituzioni comunitarie va ricavata esclusivamente dalle norme del diritto comunitario (Corte di Giustizia, 16 ottobre 1997, in e. 69-79/96; 17 settembre 1997, in e. 54/96; 6 ottobre 1981, in c. 246/80), mentre nel caso di specie essa deve essere desunta dalle disposizioni di diritto interno. Tra le due nozioni non vi è quindi necessaria coincidenza, come è confermato dalla circostanza che talvolta la Corte di Giustizia ha attribuito natura giurisdizionale anche ad organi ai quali detto carattere non era riconosciuto dai rispettivi diritti nazionali (Corte di Giustizia, 6 ottobre 1981, in c. 246/80; 17 settembre 1997, in c, 54/96; 30 giugno 1966, in c. 61/65)".

823 Sentenza della Corte (Quinta Sezione) del 16 ottobre 1997, Cause riunite C-69/96 a C-79/96, raccolta della giurisprudenza 1997 pagina I-05621 e ss, consultabile su http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri= CELEX:61996J0069:IT:PDF.

con quella adottata in caso dalla Corte di giustizia, ai fini del ricorso ex art. 267 TFUE.

In proposito, attraverso la propria giurisprudenza, la Corte di giustizia ha mano a mano enucleato alcuni requisiti che devono essere presenti, affinché sia riconosciuta la legittimazione ad operare il suddetto rinvio: "l'origine legale dell'organo [remittente], il suo carattere permanente, l'obbligatorietà della sua giurisdizione, la natura contraddittoria del procedimento, il fatto che l'organo applichi norme giuridiche e che sia indipendente"[824].

Tra l'altro, tali requisiti sono stati talvolta interpretati con una certa elasticità. Così, ad esempio, per *la natura contraddittoria del procedimento*, il contraddittorio può essere utilmente assicurato in una fase del procedimento successiva al rinvio, come nel caso dei procedimenti cautelari, ed essere anche eventuale, come nel caso dell'emanazione di ingiunzioni di pagamento[825].

Anche il requisito dell'*indipendenza* dell'organo rimettente è stato variamente apprezzato.

La nozione di indipendenza implica innanzitutto che l'organo interessato si trovi in posizione di terzietà, rispetto all'autorità che ha adottato la decisione oggetto del ricorso[826].

In merito, sono stati ulteriormente evidenziati altri due aspetti della suddetta nozione [827].

Il primo aspetto ha carattere esterno e presuppone che l'organo sia tutelato da pressioni o da interventi dall'esterno, idonei a mettere a

[824] Fra le tante, si vedano, in particolare, sentenze 17 settembre 1997, causa C-54/96, Dorsch Consult, Racc. pag. I-4961, punto 23; 21 marzo 2000, cause riunite da C-110/98 a C-147/98, Gabalfrisa e a., Racc. pag. I-1577, punto 33; 30 novembre 2000, causa C-195/98, Österreichischer Gewerkschaftsbund, Racc. pag. I-10497, punto 24; 30 maggio 2002, causa C-516/99, Schmid, Racc. pag. I-4573, punto 34; 12 novembre 1998, causa C-134/97, Victoria Film, Racc. pag. I-7023, punto 14. Sull'istituto del rinvio pregiudiziale e sul concetto di giurisdizione nazionale vedi fra glia altri G. TESAURO, *Diritto comunitario*, Padova, 2003, 285 ss.; P. MENGOZZI, *Istituzioni di diritto comunitario e dell'Unione europea*, Padova, 2003, 218 s; S. Bagni, *Consolidamento e innovazione nella giurisprudenza della Corte in tema di <<giurisdizione>> ai sensi dell'art. 234 CE e di libera circolazione dei lavoratori*, in Diritto pubblico comparato ed europeo, 2001, pag. 191 ss.

[825] Vedi sentenze 21 aprile 1988, causa 338/85, Pardini, Racc. pag. 2041; 14 dicembre 1971, causa 43/71, Racc. pag. 1039, consultabile anche su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:61971J0043:IT:HTML; 9 novembre 1983, causa 199/82, San Giorgio, Racc. pag. 3595; 11 dicembre 1997, Job Centre coop. a r.l., , causa 55/96, Racc. pag. I-07119, consultabile anche su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= CELEX:61996J0055:IT:HTML.

[826] Vedi, in questo senso, in particolare, sentenza 30 marzo 1993, causa C-24/92, Corbiau, Racc. pag. I-1277, punto 15 e 30 maggio 2002, causa C-516/99, Schmid, Racc. pag. I-4573, punto 36.

[827] Vedi Sentenza del 19 settembre 2006, causa 506/04 , Gazzetta ufficiale n. C 281 del 18/11/2006 pag. 11, consultabile su http://www.altalex.com/index.php?idnot=34913.

repentaglio l'indipendenza di giudizio dei suoi membri per quanto riguarda le controversie loro sottoposte[828].

Mentre, il secondo aspetto, avente carattere interno, si ricollega alla nozione d'imparzialità e riguarda l'equidistanza dalle parti della controversia e dai loro rispettivi interessi concernenti l'oggetto di quest'ultima.

"Questo aspetto impone il rispetto dell'obiettività (..) e l'assenza di qualsivoglia interesse nella soluzione da dare alla controversia all'infuori della stretta applicazione della norma giuridica. Tali garanzie di indipendenza e di imparzialità implicano l'esistenza di disposizioni, relative, in particolare, alla composizione dell'organo e alla nomina, durata delle funzioni, cause di astensione, di ricusazione e di revoca dei suoi membri, che consentano di fugare qualsiasi legittimo dubbio che i singoli possano nutrire in merito all'impermeabilità del detto organo rispetto a elementi esterni ed alla sua neutralità rispetto agli interessi contrapposti"[829].

Inoltre, nell'ordinanza ANAS, 26 novembre 1999[830], la Corte ha peraltro chiarito come in ogni caso è necessario accertare quale sia la natura specifica delle funzioni che l'organo esercita "nel particolare contesto normativo in cui è indotto a rivolgersi alla Corte".

Pertanto, secondo i giudici europei, la Corte dei conti non può operare il rinvio pregiudiziale alla Corte di giustizia quando esercita funzioni di controllo successivo "che sostanzialmente si risolvono in una funzione di valutazione e di controllo dei risultati dell'attività amministrativa", sebbene in altro contesto (quando giudica in materia di pensioni o di responsabilità erariale), la stessa svolga senza dubbio funzioni di natura giurisdizionale, ai sensi dell'art. 267 TFUE.

Tuttavia, si rileva come anche tale criterio sia stato applicato in modo piuttosto elastico nei confronti, invece, del Consiglio di Stato, in quanto, come si è già evidenziato, la Corte di giustizia lo ha ritenuto legittimato a sollevare questione pregiudiziale, in sede di ricorso straordinario al Capo dello Stato.

---

828 Vedi, in questo senso, sentenze 4 febbraio 1999, causa C-103/97, Köllensperger e Atzwanger, Racc. pag. I-551, punto 21, e 6 luglio 2000, causa C-407/98, Abrahamsson e Anderson, Racc. pag. I-5539, punto 36.

829 Sentenza del 19 settembre 2006, causa 506/04, cit.; vedi poi in questo senso sentenza Abrahamsson e Anderson, cit., punto 32.

830 C-192/98, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:61998O0192:IT:PDF.

Bene, venendo ora ad affrontare la questione della possibile legittimazione del Garante della protezione dei dati personali, si evidenzia prima di tutto la giurisprudenza intervenuta riguardo altre Autorità indipendenti.

Così la Corte di giustizia ha ritenuto legittimato il *Tribunal de Defensa de Competencia*[831], organo permanente, istituito con legge allo scopo di applicare le regole della concorrenza con un procedimento in contraddittorio[832].

Del pari, la Corte ha riconosciuto la possibilità di ricorrere in via pregiudiziale alla Commissione federale tedesca per la sorveglianza sulle aggiudicazioni degli appalti pubblici (*Vergabeüberwachungsausschuß des Bundes*)[833].

Tra l'altro, in questo caso, come per il Garante, è la stessa normativa comunitaria a prevedere l'indipendenza dell'organo istituito[834], attuata nell'ordinamento tedesco dalla legge 26 novembre 1993.

Mentre, con la recente sentenza del 31 maggio 2005[835], la Corte di Giustizia ha negato la legittimazione all'*Epitropi Antagonismou* (Commissione greca per la concorrenza)[836].

Con tale pronuncia, infatti, alla Commissione greca non è stato riconosciuto integralmente il requisito dell'indipendenza. Tale carenza è stata rinvenuta attraverso l'analisi della normativa nazionale relativa all'*Epitropi Antagonismou*.

L'art. 8, n. 1, della legge n. 703/1977 ha disposto, infatti, l'istituzione del suddetto organo, il quale funziona "come autorità indipendente", e ha previsto, quindi, un'autonomia amministrativa ed economica e per i suoi membri "un'indipendenza dal punto di vista personale e funzionale e,

---

831 Dal 2007 *Comisión Nacional de la Competencia*, vedi www.cncompetencia.es/.

832 C. 67/91, in Racc. 1992 Pag. I-04785, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:61991J0067:IT:PDF.

833 Sentenza 17 settembre 1997, causa 54/96, Racc.1997 pag. I-05603, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:61996J0054:IT:PDF.

834 La direttiva 89/665 dispone, all'art. 2, n. 8:" La nomina dei membri di tale organo indipendente e la cessazione del loro mandato sono soggette a condizioni uguali a quelle applicabili ai giudici, per quanto concerne l'autorità responsabile della nomina, la durata del loro mandato e la loro revocabilità. Per lo meno il presidente di tale organo indipendente deve avere le stesse qualifiche giuridiche e professionali di un giudice. L'organo indipendente prende le proprie decisioni all'esito di una procedura in contraddittorio e tali decisioni producono, tramite i mezzi determinati da ciascuno Stato membro, effetti giuridici vincolanti". Legge 26 novembre 1993, BGB. I pag. 1928.

835 C-53/03,in Racc. 2005 pagina I-04609, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= CELEX:62003J0053:IT:PDF.

836 Vedi http://www.epant.gr/category.php?Lang=en&id=84.

nell'esercizio delle loro funzioni, [questi] sono sottoposti solo alla legge e alla loro coscienza."

Il medesimo articolo, però, dispone anche che l'*Epitropi Antagonismou* sia "sottoposta al controllo del Ministro per lo (...) [Sviluppo]".

Inoltre, secondo la normativa quattro dei nove membri, nonché i relativi supplenti, dell'Autorità sono scelti dal Ministero dell'Interno, mentre tutti sono nominati dal Ministro dello Sviluppo con mandato di tre anni.

Anche il Presidente dell'Autorità (così come il suo supplente) viene nominato dal Ministro dello Sviluppo fra i membri *Epitropi Antagonismou*, così come con decisione dello stesso Ministro, su parere dell'Autorità, è nominato il direttore generale del segretariato, con durata della carica di tre anni rinnovabili.

Alla luce della suddetta normativa, la Corte ha ritenuto che il controllo del Ministero dello Sviluppo sia tale da influenzare l'indipendenza dell'Autorità, potendo entro certi limiti, controllare la legittimità delle decisioni dell'*Epitropi Antagonismou*.

Inoltre, la designazione dei membri e la mancanza di adeguate garanzie per la loro revoca o l'annullamento delle nomine non sembrano dar vita ad un sistema in grado di costituire "un reale ostacolo agli indebiti interventi o pressioni da parte del potere esecutivo nei confronti dei membri dell'*Epitropi Antagonismou* [corsivo dello scrivente]".

Questo comporta anche l'impossibilità di distinguere nettamente l'organo di vertice, con funzione giudicante, dall'ufficio, avente invece le funzioni istruttorie.

Infine, la Corte ha evidenziato che "un'autorità garante della concorrenza quale l'*Epitropi Antagonismou* è tenuta a lavorare in stretta collaborazione con la Commissione delle Comunità europee e ai sensi dell'art. 11, n. 6, del regolamento (CE) del Consiglio 16 dicembre 2002, n. 1/2003, concernente l'applicazione delle regole di concorrenza di cui agli articoli 81 [CE] e 82 [CE] (GU 2003, L 1, pag. 1), può essere privata della propria competenza da una decisione della Commissione."

Ebbene, poiché la Corte può essere adita solo da un organo chiamato a statuire su una controversia pendente dinanzi ad esso, nell'ambito di un procedimento destinato a risolversi in una pronuncia di carattere giurisdizionale, questo fa sì che "ogni volta che la Commissione priverà

della sua competenza un'autorità nazionale garante della concorrenza quale *l'Epitropi Antagonismou* [corsivo dello scrivente], il procedimento avviato dinanzi a quest'ultima autorità non si risolverà in una pronuncia di carattere giurisdizionale"[837].

Da quanto indicato, si evince che la giurisprudenza sul concetto di giurisdizione è tutt'altro che pacifica, sia in generale sia in occasione delle pronunce aventi ad oggetto i rinvii pregiudiziali da parte di Autorità indipendenti o di figure a queste, comunque, assimilabili.

Tra l'altro, i giudici comunitari, nel ricostruire le ipotesi di legittimazione, tendono ad applicare, talvolta, solo alcuni dei citati requisiti[838], perciò si è osservato che "l'approccio seguito (…) ha portato a tante nozioni quanti sono i singoli casi affrontati"[839].

Questo vuol dire che, in linea di massima, l'analisi delle condizioni soggettive ed oggettive del rinvio pregiudiziale è un'operazione in realtà sostanzialmente svolta attraverso la verifica delle circostanze del caso concreto.

Con riferimento alle Autorità indipendenti ciò implica una distinta valutazione anche all'interno della stessa categoria, stante la disomogeneità delle diverse figure, più volte precedentemente evidenziata.

In particolare, per quanto riguarda il Garante per la protezione dei dati personali è indubbia la sua origine legale, essendo stato istituito dalla legge n. 675 del 1996, in ottemperanza alla Direttiva comunitaria n. 95/46/Ce.

Il carattere dell'indipendenza, poi, è prescritto come si è visto dalla stessa normativa comunitaria e dopo l'entrata in vigore del Trattato di Lisbona, direttamente all'interno dei Trattati.

La stessa Corte di giustizia, inoltre, ha ribadito la necessità dell'indipendenza di queste figure anche recentemente nella già indicata

[837] Si veda però che la Corte di Giustizia ha dichiarato, invece, ricevibile una domanda di pronuncia pregiudiziale posta da un'autorità per la concorrenza con caratteristiche molto simili a quella greca, il già citato Tribunal de Defensa de la Competencia, C-67/91, cit.. Per quanto riguarda la motivazione relativa alla possibilità di intervento della Commissione, relativa non solo all'Autorità greca, me estesa dai giudici anche alle altre Autorità garanti della concorrenza, si rinvia alla critica di S. MENTO, *Autorità indipendenti e rinvio pregiudiziale*, in Giornale di diritto amministrativo, n. 12/2005 e A. CELOTTO (commento di), *Ma le autorità indipendenti davvero non integrano la nozione di .giurisdizione. ai fini dell'art. 234 TCE?*, in Giustizia amministrativa, 2005, pp. 903-906.

[838] Oppure ritenere alcuni requisiti non assoluti. Ad esempio, la Corte di Giusitizia nella sentenza *Dorsch Consult* (causa C-54/96 cit.), ha stabilito che non tutti i detti requisiti hanno carattere assoluto: "Va ricordato che il requisito del procedimento in contraddittorio non è un criterio assoluto.".

[839] Così S. MENTO, *Autorità indipendenti e rinvio pregiudiziale*, op. cit.

sentenza del 9 marzo 2010, nei confronti delle leggi dei Länder tedeschi, ritenendo che: "La garanzia dell'indipendenza delle autorità nazionali di vigilanza è diretta ad assicurare l'efficacia e l'affidabilità del controllo del rispetto delle disposizioni in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali e deve essere interpretata alla luce di tale finalità. Essa non è stata disposta al fine di attribuire uno status particolare a dette autorità ed ai loro agenti, bensì per rafforzare la protezione delle persone e degli organismi interessati dalle loro decisioni. Ne discende che, nello svolgimento delle loro funzioni, le autorità di controllo devono agire in modo obiettivo ed imparziale. A tale fine esse devono essere sottratte a qualsiasi influenza esterna, compresa quella, diretta o indiretta, dello Stato o dei Länder, e non solamente essere poste al riparo dall'influenza degli organismi controllati" [840].

Nel diritto interno questa è garantita dal D.lgs. n. 196/2003, secondo il quale "il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione", è organo collegiale, composto da 4 membri, eletti due dalla Camera e due dal Senato con voto limitato. Come note, poi, il Presidente è eletto direttamente dal collegio ed è previsto un sistema di incompatibilità per i membri, volto ad assicurare l'indipendenza del collegio da indebite interferenze. Al Garante è riconosciuta, poi, autonomia organizzativa, amministrativa e contabile[841].

Quanto all'attività del Garante, l'Esecutivo non ha poteri di controllo né il potere di emanare atti di indirizzo politico-amministrativo, in grado di vincolare l'Autorità al perseguimento di un obiettivo stabilito.

In particolare, riguardo l'attività decisoria del Garante si è mostrato come questa sia strutturata nelle forme di un procedimento contenzioso con elementi distintivi molto simili a quelli di un processo: è assicurato il contraddittorio fra le parti, l'Autorità ha rilevanti poteri cautelari e istruttori ed è in posizione *super partes* rispetto agli interessi in conflitto (anche se non

[840] Sentenza del 9 marzo 2010, causa C-518/07, GUUE C 113/4 del 1 maggio 2010, cit.

[841] cfr art 156 D.lgs. 196/2003, regolamenti del Garante 1/2000, cit., sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, n. 2/2000, cit, concernente il trattamento giuridico ed economico del personale del Garante , n. 3/2000, cit, sulla gestione amministrativa e contabile. Cfr anche L. CERRONI, in C.M. BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d.lgs. 30 giugno 2003, n. 196 (<<Codice della privacy>>)*, op. cit. pag. 2001 e ss.

è terza nel senso proprio del giudice), ovvero è equidistante dalle parti, pubbliche o private, e dai loro rispettivi interessi.

Inoltre, per la risoluzione della controversia applica, seppur con margini interpretativi talvolta ampi, la normativa in materia di trattamento dei dati personali, anche quella comunitaria, secondo quanto previsto dalla disciplina nazionale, nonchè dai Trattati e dalla Carta dei diritti fondamentali dell'Unione europea.

Come precedentemente illustrato, poi, la tutela giustiziale amministrativa di fronte al Garante è alternativa rispetto a quella giurisdizionale. Tale caratteristica, quindi, è prevista in termini molto più forti di quella del ricorso straordinario al Capo dello Stato, nel quale è riconosciuta la possibilità di trasposizione della controversia davanti al giudice.

Infine, i provvedimenti del Garante sono obbligatori, immediatamente esecutivi - persino l'opposizione davanti al giudice ordinario non ne sospende automaticamente l'esecutività- e assistiti da sanzione penale nel caso di inosservanza.

Dunque, tirando infine le somme, tutti i suddetti elementi messi a confronto con quanto emerso in merito al requisito di "giurisdizione nazionale", rilevante ai fini della legittimazione a sollevare questione pregiudiziale ai sensi dell'art 267 del TFUE, sembrerebbero invero condurre a propendere, con tutte le cautele del caso, per il riconoscimento in capo al Garante per la protezione dei dati personali, quando esercita funzione giustiziale[842], della possibilità di bussare anche alla porta della Corte di giustizia. A quest'ultima, però, non può che essere riservata l'ultima parola in merito.

[842] Potrebbe discutersi se la stessa legittimazione sussista anche nell'ambito dei procedimenti iniziati d'ufficio o su segnalazione e reclamo da parte degli interessati, rientrando questi nell'attività generale di vigilanza dell'Autorità più propriamente amministrativa, anche se questa viene comunque esercitata dall'Autorità con la medesima indipendenza e imparzialità, in contraddittorio fra le parti e può portare all'adozione di provvedimenti obbligatori ed esecutivi.

CONCLUSIONI

Le considerazioni, esposte in questa analisi del rapporto fra privacy e nuove tecnologie nel sistema socio-giuridico moderno e di alcune delle maggiori questioni ad esso connesse, hanno voluto mettere in evidenza, in particolare, la trasversalità dell'argomento.

La materia, infatti, non solo è in grado di incidere sullo sviluppo della persona, sia come singolo sia nelle formazioni sociali con cui questa si relaziona, ma attraverso l'incessante progresso tecnologico, gli stessi processi democratici sono influenzati dal modo in cui circolano le informazioni.

Così, si è inizialmente illustrata la lunga evoluzione del concetto di privacy, dall'originaria definizione come diritto ad essere lasciati da soli sino al diritto di mantenere il controllo sulle proprie informazioni.

La tutela dei dati personali è diventata in tal modo un vero e proprio diritto fondamentale, riconosciuto espressamente nella Carta dei diritti fondamentali dell'Unione europea e, con l'entrata in vigore del Trattato di Lisbona, anche nel Trattato sull'Unione europea e nel Trattato sul funzionamento dell'Unione europea.

Si messo poi in evidenza come gli strumenti di tutela della privacy e dei dati personali debbano essere adeguati all'evoluzione delle innovazioni tecnologiche, risultando, pertanto, strutturalmente dinamici. Tale evoluzione finisce per coincidere con il generale processo di globalizzazione della società moderna.

In seguito, si sono analizzati alcuni rischi legati ad uno sviluppo incontrollato delle applicazioni tecnologiche in determinati settori, mettendo in evidenza la necessità di lavorare perché queste si coordinino sempre con i principi e i diritti fondamentali, così da poter parlare di una "tecnologia virtuosa".

Un ruolo fondamentale avranno in questa direzione la politica ed il legislatore, tuttavia, poiché si è visto che la questione è inserita ormai in un contesto globale, non potrà trattarsi di una fonte legislativa monocentrica, bensì di "un policentrismo di fonti collocate in una coordinata sequenza di vari livelli (una cornice legislativa concertata tra tutti i Paesi interessati alla soluzione del problema e, in aderenza ad essa, la specificazione di regole

mediante leggi nazionali, a seconda delle varie aree geografiche, e inoltre l'adozione di codici-modello di formazione autodisciplinare)"[843].

Sarà, poi, indispensabile che nella definizione di queste strategie siano coinvolti sin dall'inizio esperti di tecnologie, per aiutare ad indirizzare correttamente le scelte iniziali e valutarne gli impatti.

Si deve tenere presente, infatti, che nella moderna rivoluzione informatica ormai sono davvero poche le attività che possono essere svolte senza il coinvolgimento di esperti in tecnologie.

Un altro aspetto fondamentale che si è cercato di porre in evidenza è il ruolo che dovrebbe avere l'educazione alla tecnologia: un uso consapevole della tecnologia è la prima forma di tutela verso i possibili abusi.

E' stato rilevato, ancora, come la tutela dei diritti della personalità, fra cui la privacy, sia direttamente proporzionale e non ostativa alla diffusione delle tecnologie, di cui il cittadino fa ancora poco uso proprio per paura di subirne lesioni. Solo se le persone si sentiranno sicure dell'uso corretto dei propri dati si avvantaggeranno delle innovazioni tecnologiche.

Inoltre, si è indicato come sia la normativa comunitaria che quella nazionale sulla protezione dei dati personali ruotino intorno alla figura forte di un'Autorità indipendente.

Quindi, nella definizione degli equilibri fra i diversi interessi coinvolti nel caso concreto soprattutto dove, come nelle tecnologie di ultima generazione, ancora non sussiste un adeguato supporto normativo, un ruolo di vero e proprio baricentro sarà (ed è tuttora) svolto dal Garante per la protezione dei dati personali.

Decisivo sarà, peraltro, anche il ruolo dei giudici che nell'applicazione del diritto al caso concreto dovranno ricavare la regola giuridica o il principio da applicare.

Pertanto, nell'analisi del rapporto fra privacy e società globale si è ritenuto di dover svolgere alcune osservazioni sulla figura del Garante per la protezione dei dati personali.

Su di essa e su talune questioni legate in generale alle Autorità indipendenti, quindi, ci si è soffermati nell'ultimo capitolo, analizzando le conseguenze che l'inquadramento delle funzioni dalle stesse esercitate può

[843] Così G. SANTANIELLO, *Tipologia delle innovazioni tecnologiche e protezione dei dati personali,* op. cit.

avere sull'assetto complessivo istituzionale e sulla giustizia costituzionale in particolare.

Non si sono omesse, poi, alcune riflessioni anche in riguardo l'ordinamento comunitario, relative alla possibilità di proporre ricorso pregiudiziale alla Corte di giustizia da parte del Garante per la protezione dei dati personali, data l'incidenza che la suddetta normativa ha nella definizione del ruolo, dei poteri e delle competenze dell'Autorità.

Infine, per concludere si riportano le parole di Stefano Rodotà, le quali rappresentato non solo la miglior sintesi, ma anche, in un certo senso, lo stesso filo conduttore delle osservazioni svolte nel presente lavoro, con il quale si è cercato di far emergere in un quadro d'insieme le diverse dimensioni che il diritto alla privacy assume nella società globale.

"Senza una forte tutela delle informazioni, le persone rischiano sempre di più d'essere discriminate per le loro opinioni, credenze religiose, condizioni di salute: la privacy si presenta come un elemento fondamentale della <<società dell'eguaglianza>>. Senza una forte tutela dei dati riguardanti i loro rapporti con le istituzioni o l'appartenenza a partiti, sindacati, associazioni, movimenti, i cittadini rischiano d'essere esclusi dai processi democratici: così la privacy diventa una condizione essenziale per essere inclusi nella <<società della partecipazione>>. Senza una forte tutela del <<corpo elettronico>>, dell'insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo e si rafforzano le spinte verso la costituzione di una società della sorveglianza, della classificazione, della selezione sociale: diventa così evidente che la privacy è uno strumento necessario per salvaguardare la <<società della libertà>>. Senza una resistenza continua alle microviolazioni, ai controlli continui, capillari, oppressivi o invisibili che invadono la stessa vita quotidiana, ci ritroviamo nudi e deboli di fronte a poteri pubblici e privati: la privacy si specifica così come una componente ineliminabile della <<società della dignità>>"[844].

Il compito del giurista in generale e dello studioso del diritto costituzionale in particolare può essere ricondotto, allora, proprio a quello

[844] In *Intervista su Privacy e libertà*, op. cit., pag. 148-149.

di coscienza vigile dei diritti inviolabili nella società globale dell'informazione e della rivoluzione tecnologica[845] .

[845] Cfr A PUNZI, *La persona nei dati. Ragioni e modelli di una regolamentazione*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Il codice del trattamento dei dati personali, op. cit.

BIBLIOGRAFIA

F. G. ANGELINI, *Pubblica amministrazione digitale, diritto di accesso e privacy*, in L. BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, RCS Etas, Milano, 2010, pag 260.

G. AMATO, *Le Autorità indipendenti nella Costituzione economica*, in AA.VV., Regolazione e garanzia del pluralismo. Le Autorità Amministrative indipendenti, Giuffrè, Milano pag 16.

G. AMATO, *Autorità semi – indipendenti ed Autorità di garanzia*, in Rivista trimestrale di diritto pubblico, 1997, pag. 653.

G. ARIETA, *Art. 29*, in La tutela dei dati personali. Commentario alla l. n. 675/1996, diretto da E. GIANNANTONIO, M.G. LOSANO e V. ZENO ZENCOVICH, Padova, Cedam, 1997, pag. 382.

M. ATELLI, *Chiamate indesiderate. Commento*, in AAVV, Privacy e telecomunicazioni. Commentario al D.lgs. n 172 /1998, Napoli, 1999.

T. A. AULETTA, *Riservatezza e tutela della personalità*, Giuffrè, Milano, 1978, pag 51.

S. AXELRAD, *Survey of State DNA Database Statutes*, in American Society of Law, Medicine, and Ethics, consultabile in http://www.aslme.org/dna_04/grid/guide.pdf.

A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, Bulzoni, Roma, 1974.

A. BALDASSARE, *Diritti della persona e valori costituzionali*, Giappichelli, Torino, 1997.

E. BALLACCI, *UE, Reding: "Contraria ai body scanner, urgono verifiche"*, articolo consultabile su http://www.newnotizie.it/2010/01/13/ue-reding-contraria-ai-body-scanner-urgono-verifiche/

T. BALLARINO, *Internet nel mondo della legge*, Cedam, Padova 1998.

T. BALLARINO, *Diritto internazionale privato*, Cedam, Padova 1999.

A. BARBERA, *Commento all'art. 2 della Costituzio*ne, in G. BRANCA (a cura di), Commentario della Costituzione, Zanichelli, Bologna, 1975.

A. BARBERA, "*Nuovi diritti": attenzione ai confini*, in L. CALIFANO (a cura di), Corte costituzionale e diritti fondamentali, Giappichelli, Torino 2004, p. 19 ss.

M. BARBERA, *I principi costituzionali della libertà personale*, Giuffrè, Milano, 1967.

R. BARESI, *La sicurezza informatica, una nuova sfida per il mondo bancario*, consultabile su http://www.01net.it/articoli/0,1254,1_ART_78205,00.html.

S. BARTOLE, *Corte e Diritti*, in Corte costituzionale e sistema istituzionale, Convegno dell'Associazione Gruppo di Pisa, (Pisa 4-5 giugno 2010), in corso di pubblicazione in Quaderni del Gruppo di Pisa, Giappichelli, Torino, 2011.

S. BARTOLE *Per la Corte costituzionale le coppie omosessuali sono formazioni sociali, ma non possono accedere al matrimonio*, in Foro it., 2010, I, 1367.

S. BARTOLE, *Il diritto "consentito" al matrimonio ed il diritto "garantito" alla vita familiare per le coppie omosessuali in una pronuncia in cui la Corte dice "troppo" e "troppo poco"*, in Giur. cost., 2010, fasc. 2.

E. BASSOLI, *E-Government e privacy*, consultabile in www.federalismi.it.

A. BELVEDERE, *Riservatezza e strumenti d'informazione*, in Dizionario del dir. priv., Milano, 1980, p. 750.

J. BENTHAM, *Panopticon* ,1797, trad. it. di V. FORTUNATI, Padova, 1983.

M. BESSONE, G. FERNANDO, *v. Persona fisica. a) Diritto Privato*, Enc. Dir, 1983, pag 209.

G. BERTI, *Amministrazione e Costituzione*, Dir. Amm., 1993, pag 465.

P. BIANCHI, *Il conflitto di attribuzioni fra Stato e Regione e tra regioni*, in R. ROMBOLI (a cura di), Aggiornamenti in tema di processo costituzionale (2005-2007), Giappichelli, Torino, 2008.

P. BIANCHI, E. MALFATTI, *L'accesso in via incidentale*, in A. ANZON, P. CARETTI, S. GRASSI (a cura di) Prospettive di accesso alla giustizia costituzionale, Giappichelli, Torino, 2000, pag. 24.

G. BIANCHINI, *La sfera della privacy nell'era digitale: minacce e mezzi di difesa*, consultabile su www.giannibi.net/nottebianca.pdf.

F. BILANCIA, *La crisi dell'ordinamento giuridico dello Stato rappresentativo*, Cedam, Padova, 2000, pag 13-14 , 131, 331 ss.

P. BILANCIA, *Attività normativa delle autorità indipendenti e sistema delle fonti*, in S. LABRIOLA, Le Autorità indipendenti, Giuffrè, Milano, 1999 , pag 157.

R. BIN, *Diritti e argomenti. Il bilanciamento degli interessi nella giurisprudenza costituzionale*, Giuffè, Milano, 1992, 81.

R. BIN, *Ragionevolezza e divisione dei poteri*, in Diritto & Questioni pubbliche, 2, 2002, pag. 123, consultabile su www.dirittoequestionipubbliche.org.

P. BISCARETTI di RUFFIA (a cura di), con la collaborazione di M. GANINO, *Costituzioni straniere contemporanee*, vol. II: Le Costituzioni di sette Stati di recente ristrutturazione, VI ed. interamente rifatta, Giuffrè, Milano 1996, 25 ss.

E. J. BLOUSTEIN, *Privacy as an aspect of human dignity: an answer to Dean Prosser*, in N.Y.U. L. Rev., 1964.

L. BOLOGNINI, D. FULCO, P. PAGANINI, L. SCUDIERO, *Cloud computing e protezione dei dati personali: privacy e web globale, rischi e risorse*, in L BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, RCS Etas, Milano, 2010, pag 33.

L. BOLOGNINI e P. PAGANINI, *La libertà di Internet e reati: sì all'anonimato protetto*, consultabile su http://mediablog.corriere.it/2009/12/liberta_di_internet_e_reati_si.html.

L. BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), *Next Privacy*,RCS Etas, Milano, 2010.

L. BOLOGNINI e G. FORGESCHI, La *next privacy nella sanità digitale italiana*, in L BOLOGNINI, D. FULCO, P. PAGANINI, Next Privacy, RCS Etas, Milano, 2010, pag. 219.

F. BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in AAVV, Il diritto alla riservatezza e la sua tutela penale, Atti del terzo simposio di studi di diritto e procedura penali, Varenna, Villa Monastero, 5-7 settembre 1967/ promosso dalla Fondazione "Avv. Angelo Luzzani" di Como - Giuffrè, Milano, 1970 , pag 80.

F. BRUGALETTA – F. M. LANDOLFI (a cura di), *Il Diritto nel Cyberspazio*, Simone, 1999.

H. BURKERT, *Privacy Enhancing Technologies: Typology, Critique, Vision*, in P. E. AGRE and M. ROTENBERG (eds.) Technology and privacy: the new landscape, Cambridge Mass. MIT Press 1998, cap. IV, consultabile su http://cognet.mit.edu/library/books/mitpress/0262511010/cache/chpt4.pdf.

G. BUTTARELLI, Convegno "Carta di identità elettronica e firma digitale: dalla sperimentazione ai servizi", 2002, http://www.garanteprivacy.it/garante/doc.jsp?ID=45900.

D. CALDIROLA, *Il diritto alla riservatezza*, Cedam, 2006.

A. CALMIERI, R PARDOLESI., *Il codice in materia di protezione dei dati personali e l'intangibilità della "privacy" comunitaria*, in Il Foro It., 2004, IV, pp. 57- 64, consultabile anche su http://www.law-economics.net/public/Palmieri_%20e%20Pardolesi%20_sul%20caso%20Lindqvist.pdf.

E. L. CAMILLI, M CLARICH, *Poteri quasi giudiziali delle autorità indipendenti*, nota elaborata per il gruppo di lavoro Astrid "La riforma delle Autorità indipendenti", consultabile su http://www.astrid-online.it/Riforma-de3/Contributi/Camilli_Clarich_gruppo_AI.pdf.

F. CARINGELLA, *Corso di diritto amministrativo*, Giuffrè, Milano2004, p. 885.

F. CARINGELLA, *La Misteriosa identità delle autorità indipendenti: pubbliche amministrazioni speciali o espressione di un quarto potere acefalo e vagamente mostruoso?*, in Lezioni e Sentenze di diritto amministrativo 2007, ildirittopericoncorsi, 2007.

A. CARLO, *La proiezione costituzionale della banca dati italiana del DNA per finalità di indagine criminale. Riflessioni a margine dei progetti di legge presentati nel corso della XV legislatura,* in C. CASONATO C., PICIOCCHI, P. VERONESI (a cura di), Forum biodiritto 2008 La circolazione dei modelli nel biodiritto, Cedam, 2009.

L. CASETTI, *la cultura del mercato fra interpretazioni della Costituzione e principi comunitari*, Giappichelli, Torino, 1997, pag. 353.

C. CASONATO, *Bioetica e pluralismo nello Stato Costituzionale*, consultabile in www.forumcostituzionale.it.

G. CASSANO, *Il diritto all'oblio esiste: è diritto alla riservatezza* (nota a Trib. Roma 15 maggio 2005), in Il diritto di famiglia e delle persone, 1998.

G.CASSANO, *Il diritto alla riservatezza fra dottrina e giurisprudenza*, in www.studiocelentano.it.

C. CASONATO, *La discriminazione genetica: una nuova frontiera nei diritti dell'uomo?*, in Atti del XV Convegno AIDC, Messina – Taormina, 2001, p. 2 ss.

S. CASSESE, *Negoziazione e trasparenza nei procedimenti davanti alle Autorità indipendenti*, in Il procedimento davanti alle Autorità indipendenti, Quaderni del Consiglio di Stato, Torino, 1999, pag 42

S. CASSESE, C. FRANCHINI (a cura di), *I garanti delle regole. Le Autorità Indipendenti*, Il Mulino, Bologna, 1996

G. CATALDI, *La Convenzione del Consiglio d'Europa sui diritti dell'uomo e la biomedicina*, in L. CHIEFFI (a cura di), Bioetica e diritti dell'uomo, Torino, Paravia-Mondadori, 2000, p. 267 ss.

A. CATAUDELLA, *La tutela civile della vita privata*, Giuffrè, Milano, 1972, pag 32.

F. CECAMORE, *L'autorità indipendente come giudice a quo nel giudizio costituzionale*, in R. BALDUZZI, P. COSTANZO (a cura di), Le zone d'ombra della giustizia costituzionale. I giudizi sulle leggi, Giappichelli, Torino, 2007, pag. 97 e ss.

A. CELOTTO, *La prevalenza del Diritto comunitario sul Diritto degli Stati: ambito e portata della disapplicazione*, in http://www.iidpc.org/revistas/8/pdf/129_145.pdf.

A. CELOTTO (commento di), *Ma le autorità indipendenti davvero non integrano la nozione di giurisdizione. ai fini dell'art. 234 TCE?*, in Giustizia amministrativa, 2005, pp. 903-906.

A. CENICCOLA, *Il diritto di accesso dopo la legge n. 15/2005*, consultabile in www.lexitalia.it.

P. CERINA, *Il problema della legge applicabile e della giurisdizione*, in E. TOSI (a cura di), I problemi giuridici di Internet, Giuffrè Milano, 1999, pag. 351 ss.

A. CERRI, *Libertà negativa di manifestazione del pensiero e di comunicazione - diritto alla riservatezza: fondamento e limiti*, in Giur. Cost., 1974, I, pag. 611 e ss.

A. CERRI, *Regime delle questue: violazione del principio di uguaglianza e tutela del diritto alla riservatezza*, in Giur. Cost. 1972.

A. CERRI, *voce Riservatezza (diritto alla), III) Diritto comparato e straniero*, in Enc. Giur. Treccani, Istituto Poligrafico e Zecca dello Stato, Roma 1995.

L. CERRONI, in C.M. BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d.lgs. 30 giugno 2003, n. 196 (<<Codice della privacy>>)*, Cedam, Padova, pag. 2001 e ss.

V. CERULLI IRELLI - *Osservazioni generali sulla legge di modifica della L. n. 241/*90 - I parte, in www.giustamm.it, Speciale sulla riforma della L.241/1990.

E. CHELI, *Intervento,* in ISLE, Disciplina generale delle Autorità indipendenti, in Rass. Parl., 1999, pag 927 e ss.

E. CHELI, *Parlamento e autorità indipendenti*, in Associazione italiana dei costituzionalisti, Annuario 2000, Il Parlamento, atti del XV Convegno annuale Firenze 12-14 ottobre 2000, Cedam, Padova, 2001, pag.323-324.

L. CHIEFFI, *Analisi genetica e tutela del diritto alla riservatezza. Il bilanciamento tra il diritto di conoscere e quello di ignorare le proprie informazioni biologiche*, consultabile su http://www.associazionedeicostituzionalisti.it/dottrina/libertadiritti/Chieffi.pdf.

L. CHIEFFI, *Ingegneria genetica e valori personalistici*, in L. CHIEFFI (a cura di), Bioetica e diritti dell'uomo, Paravia – Mondadori,Torino, 2000.

R. CHIEPPA, *Tipologie procedimentali e contradditorio davanti alla Autorità indipendenti,* consultabile su www.giustizia-amministrativa.it, pag 3.

F. CINTOLI, *I regolamenti delle Autorità indipendenti nel sistema delle fonti tra esigenze della regolazione e prospettive della giurisdizione*, in giustizia-amministrativa.it, 2003.

G. P. CIRILLO, *Diritto all'accesso e diritto alla riservatezza: un difficile equilibrio mobile*, in www.giustizia-amministrativa.it.

G.P. CIRILLO, *La tutela in via amministrativa del trattamento dei dati personali*, G. SANTANIELLO (cura di), La protezione dei dati personali, Cedam, Padova, 2005, pag. 739.

G.P. CIRILLO, *Il nuovo codice in materia di trattamento dei dati e gli schemi di riferimento relativi alla tutela dei diritti fondamentali della persona e dei cd. diritti dell'interessato*, in G. SANTANIELLO (a cura di), La protezione dei dati personali, Cedam, Padova, 2005.

G.P. CIRILLO e R. CHIEPPA (a cura di), *Le autorità amministrative indipendenti*, in Trattato di diritto amministrativo, vol. 41, Cedam, Padova, 2010 pag. 557.

M. CLARICH, *I procedimenti di regolazione*, in AA.VV., Il procedimento davanti alle autorità indipendenti, Giappichelli, Torino, 1999 pag. 19.

M. CLARICH, *Trasparenza e diritti della personalità nell'attività amministrativa*, intervento al Convegno "Trasparenza e protezione dei dati personali nell'azione amministrativa", Roma, 11 febbraio 2004, in www.giustizia-amministrativa.it.

M. CLARICH, G. CORSO, V. ZENO-ZENCOVICH, *Le autorità indipendenti: un catalogo delle questioni aperte*, atti del Convengo Il sistema delle Autorità indipendenti: problemi e prospettive, Roma 27 febbraio 2006, consultabile su eprints.luiss.it/128/1/Clarich_2006_01_OPEN.pdf.

G. COMANDé, *Commento all'art. 18*, in C.M. BRANCA , F.D. BUSNELLI (a cura di), Tutela della privacy, in Le nuove leggi commentate, 1999.

T. M. COOLEY, *Treatise on the law of Torts or the Wrongs Which Arise Independently of Contract*, del 1878, pubblicato da Callaghan & Company, 1907, consultabile su http://www.archive.org/details/cu31924019311426.

P. COPPOLA, in La Repubblica, 11 agosto 2007.

P. CORSINI, E. ORBINI MICHELACCI, *Sostituire il documento cartaceo con il documento informatico, firmarlo e trasmetterlo in rete*, in "Diritto dell'Internet", Ipsoa, n. 3/2006, p. 311.

F. COSTANTINI, *Sulla natura del Garante per la protezione dei dati personali*, nota a Cassazione Civile, Sez. Ia, 20 maggio 2002, n. 7341, consultabile su http://www.filosofiadeldiritto.it/NUOVO%20ARCHIVIO/CostantiniGiur2-03%20NUOVO.htm.

L. COZZOLINO, *Le tradizioni costituzionali comuni nella giurisprudenza della Corte di giustizia delle Comunità europee*, consultabile su http://www.associazionedeicostituzionalisti.it/materiali/convegni/copanello020531/cozzolino.html.

G. CREA, *La protezione dei dati personali tra diritti d'impresa, dei consumatori, della concorrenza*, in L. BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, RCS Etas, Milano, 2010, 138 e ss.

V. CRISALFULLI, L. PALADIN, *Commentario breve alla Costituzione*, Cedam, Padova, 1990.

J. CUERVO, *Autodeterminación Informativa*, consultabile su http://www.informatica-juridica.com/trabajos/autodeterminacion_informativa.asp.

A. D'ALOIA, *Introduzione. I diritti come immagini in movimento: tra norma e cultura costituzionale*, in A. D'ALOIA (a cura di), Diritti e Costituzione, Profili evolutivi e dimensioni inedite,Giuffrè, Milano, 2003.

B. DALLA PICCOLA, *I test genetici: panoramica generale*, consultabile su www.privacy.it/dallapiccola20020321.html.

G. DAL SASSO, *Rispetto della dignità della persona e tutela della privacy, particolarmente in sanità*, consultabile su www.formazione.eu.com/ documents/casagrande/articoli/2004-03-08/articolo.pdf.

P. DE CAROLIS, *Schedatura del Dna, l'Islanda si ribella*, in Il Corriere della Sera 17 maggio 2004.

A. DE CUPIS, *I diritti della personalità* , Vol.I, Giuffrè, Milano, 1973.

C. DE GIACOMO, *Diritto, libertà e Privacy nel mondo della comunicazione globale*, Giuffrè, Milano, 1999, pag 5 e 16.

C. DE FIORES, *Il fallimento della Costituzione europea. Note a margine del Trattato di Lisbona*, in http://www.costituzionalismo.it/articolo.asp?id=272.

G. DE MINICO, *Cambia l'oggetto del potere regolamentare delle Autorità Indipendenti a seguito della riforma del Titolo V della Parte II della Costituzione*, in Forum di Quad. cost., 2003.

U. DE SIERVO, *Le diversità fra le varie Autorità*, in Autorità indipendenti e principi costituzionali. Atti del Convegno di Sorrento 30 maggio 1997, Cedam, Padova, 1999, pag 71.

U. DE SIERVO, *Recenti sviluppi della giurisprudenza della Corte costituzionale in relazione alla giurisprudenza della Corte europea dei diritti dell'uomo*, consultabile su http://www.cortecostituzionale.it/informazione/file/19_21_11_09_De%20Siervo_2.pdf.

S. DELLA VALLE, *Una legge fondamentale post-costituzionale? Il diritto pubblico europeo alla luce del Trattato di Lisbona*, consultabile su www.costituzionalismo.it.

A. DEL NINNO, *Geolocalizzazione: le sfide alla privacy nella società del controllo globale*, in L. BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, RCS Etas, Milano, 2010, pag 97 e ss.

C. DI GIORGIO, *AAA in Islanda è in vendita il Dna*, 13 gennaio 1999, in http://www.repubblica.it/online/cultura_scienze/islanda/islanda/islanda.html.

A. DI MARTINO, *La protezione dei dati personali*, in S. P. PANUNZIO (a cura di), I diritti fondamentali e le corti in Europa, Jovine, Napoli, 2005 pag. 386 e ss.

R. D'ORAZIO, in GIANNANTONIO, LOSANO, ZENO-ZENCOVICH (a cura di), *La tutela dei dati personali, Commentario alla l. 675/1996*, Padova, pag 302.

A. DIX, Le tecniche Rfid, in Innovazioni tecnologiche e privacy, consultabile su www.garanteprivacy.it.

A. DUFF, *Guida al Trattato di Lisbona*, consultabile su http://www.andrewduffmep.org.uk/resources/sites/217.160.173.25406d96d1812cb6.84417533/EU%20Constitution%20Briefing/Guida+al+trattato+Italiano.pdf.

R. DULBECCO, in LeScienze, aprile 2007.

F. DURANTE, *La legittimazione delle autorità indipendenti ad essere parte nei conflitti di attribuzione*, consultabile su http://www.ambientediritto.it/dottrina/Dottrina%202004/legittimazione_autorita_indipendenti_durante.htm.

P. DURET, *Autorità ed Agenzie e l'amministrazione in cammino*, in P. CAVALERI, G. DALLE VEDOVE, P. DURET (a cura di), Autorità indipendenti e Agenzie. Una ricerca giuridica interdisciplinare, Padova, Cedam, 2003, pag. 36.

M. ESPOSITO, *Si aprono le «porte del cielo»: dall'arbitrato al ricorso straordinario al Presidente della Repubblica?*, in Giur. Cost., 2001, 3768 e ss

N. FABIANO, *Internet of things: il fenomeno e le prospettive giuridiche*, in L. BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, RCS Etas, Milano, 2010, pag.91.

N. FABIANO, *La lotta ai furti di identità nel Web 2.0*, in L BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, RCS Etas, Milano, 2010, pag. 68 e ss.

L. M. FALCO, *Computer portatili agli studenti ma la scuola li spiava in casa*, su La Repubblica del 20 febbraio 2010, consultabile su http://www.repubblica.it/scuola/2010/02/20/news/scuola_usa_spia-2374378/.

G. FALCON, *il "primo", il "secondo" ed il "terzo" garante*, in Mercati e amministrazioni indipendenti, F. Bassi, F. Merusi *(*A cura di), Giuffrè, Milano, 1993, pag 96.

G. FAMIGLIETTI, *Il diritto alla riservatezza o la riservatezza come diritto. Appunti in tema di riservatezza ed intimidad sulla scorta della giurisprudenza della Corte costituzionale e del Tribunal Constitucional*, consultabile su http://www.forumcostituzionale.it/site/index3.php?option=content&task=view&id=212.

G. FERRANDO, *Profili giuridici dei test genetici e decisioni riproduttive*, consultabile su www.privacy.it/ferrando2002032.html.

G.B. FERRI, *Diritto all'informazione e diritto all'oblio*, in "Rivista di diritto civile", 1990.

G.B. FERRI, *Persona e privacy*, in Riv. Dir. Comm., 1982, I.

A. FERRUCCI, *Diritto di accesso e riservatezza: osservazioni sulle modifiche alla l. 241/90*, consultabile su http://www.giustamm.it/new_2005/ART_2005.htm.

F. FIGORILLI, *La tutela amministrativa*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Giappichelli, Torino, 2007, pag. 679 e ss.

C. FILIPPI, *Le nuove regole per i servizi di comunicazione elettronica:l'attuazione della direttiva 2002/58. La tutela della riservatezza su internet e reti telematiche*, in G. SANTANIELLO (a cura di) La protezione dei dati personali, Cedam, Padova, 2005, pag 617.

G.M. FLICK, *Prefazione*, in G. SANTANIELLO (a cura di), La protezione dei dati personali, Cedam, Padova, 2005.

S. FOIS, *Questioni sul fondamento costituzionale del diritto all'<<identità personale>>*, in AAVV, L'informazione e i diritti della persona, Jovene, Napoli, 1983, pag 167.

C. FRANCHINI, *Le autorità indipendenti come figure organizzative nuove*, in S. CASSESE, C. FRANCHINI (a cura di), I garanti delle regole, Le Autorità Indipendenti, Il Mulino, Bologna, 1996.

M. FRANZONI, *dati personali e responsabilità civile*, in Responsabilità civile e previdenza, 1998.

C. FRIED, *Privacy*, in Yale L. Rev, J. 1968, 77, 482.

T. E. FROSINI, *Diritto alla riservatezza e calcolatori elettronici*, in G. ALPA e M. BESSONE (a cura di), Banche-dati e diritti della persona, Cedam, Padova, 1984.

T. E. FROSINI, *Libertà informatica:brevi note sull'attualità di una teoria giuridica*, consultabile su http://www.dirittoestoria.it/7/Contributi/Frosini-Libert-informatica.htm#_ftn3.

T. E. FROSINI, *Tecnologie e libertà costituzionali*, G. COMANDE' e G. PONZALLI (a cura di) in Scienza e diritto nel prisma del diritto comparato, Giuffrè, Milano, 2004, pag 179 e ss.

T. E. FROSINI, *Libertà informatica come libertà costituzionale*, in Materiale selezionato dal corso di Informatica e diritto P.O.R. Campania, consultabile su http://www.unisob.na.it/e-unisob/eteca/innovazione/innovazione_4 /innovazione_4_12.pdf.

V. FROSINI, *L'orizzonte giuridico dell'Internet*, in Il diritto dell'informazione e dell'informatica, n. 2, 2002, pag. 275.

D. FULCO, *La protezione dei dati personali. Diritti e strumenti di tutela*, in M. SGROI (a cura di) , Nuovi ambiti di tutela della personalità, Giappichelli, Torino, 2007.

E. FURNO, *Corte costituzionale e arbitrati: un nuovo "giudice a quo"?*, in Giur. it., 2004, pag. 437.

S. GAINOTTI, A.G. SPAGNOLO, *Test genetici: a che punto siamo in Europa*, in Medicina e morale, 4, 2004, p. 737 ss.

M. GAMBULI, *La responsabilità penale dei provider per i reati commessi in internet*, www.altalex.com/index.php?idstr=0&idnot=9965.

G. GARBI, *L'importanza delle sentenze della Corte Europea di Giustizia nel processo di giuridificazione dei diritti della persona ed in particolare della privacy*, in Diritto e diritti - Rivista giuridica elettronica pubblicata su Internet, consultabile su www.diritto.it/archivio/1/20682.pdf.

D. GELLES, in Financial Times, consultabile su http://www.ft.com/cms/s/2/aefb5d4e-1d97-11df-a893-00144feab49a.html.

G. GEMMA, *Garante per la radiodiffusione e l'editoria e conflitti di attribuzione tra i poteri dello Stato*, in Giur. Cost., 1995, pag. 1661 e ss.

M. E. GENNUSA, *Dal Trattato Costituzionale al Trattato di Lisbona (27 febbraio 2008)*, consultabile http://economia.unipv.it/pagp/pagine_personali/gennel/materiale/Dal%20Trattato%20costituzionale%20al%20Trattato%20di%20Lisbona.doc.

G. GIACOBBE, *Competenza della Authorities e tutela dei diritti della persona*, in P. PERLINGERI (a cura di), Authorities e tutela della persona, Esi, Napoli, 1999 pag .53.

G. GIACOBBE, *Il diritto alla riservatezza nella prospettiva degli strumenti di tutela*, in AAVV, Il riserbo e la notizia. Atti del convegno di Studio. Macerata, 5-6 marzo 1982, Napoli, 1983, p. 113.

G. GIAMPICCOLO, *La tutela giuridica della persona umana e il cd. diritto alla riservatezza*, in Riv. Trim. dir. Proc. Civ., 1958, pag 465-466.

A. GINORI, Gli spazzini del passato on line, articolo pubblicato sul quotidiano La Repubblica, mercoledì 10 dicembre 2009.

R. GIORDANO, La tutela giurisdizionale, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Giappichelli, Torino, 2007, pag 713 e ss.

M. GIORGIANNI, *La tutela della riservatezza*, in Riv, trim. dir e proc. Civ., 1970.

T. GIOVANNETTI, *I «soggetti esclusi» nei conflitti di attribuzione*, in R. PINARDI (a cura di), Le zone d'ombra della giustizia costituzionale. I giudizi sui conflitti di attribuzione e sull'ammissibilità del referendum abrogativo, Atti del seminario di Modena, 13 ottobre 2006, Giappichelli, Torino, 2007.

T.F GIUPPONI, *Corte costituzionale, obblighi internazionali e "controlimiti allargati": che tutto cambi perché tutto rimanga uguale?*, consultabile su http://www.forumcostituzionale.it/

site/images/stories/pdf/documenti_forum/giurisprudenza/2007/0003_giupponi_nota_348_349_2007.pdf.

G. GRASSO, *Le Autorità amministrative indipendenti della Repubblica*, Giuffrè, 2006, pag. 5.

G. GRASSO, *Autorità amministrative indipendenti e conflitti intersoggettivi: una zona d'ombra della giustizia costituzionale?* , in Amministrazione in cammino, consultabile su http://www.amministrazioneincammino.luiss.it/wpcontent/uploads/2010/03/Intervento.pdf.

G. GRASSO, *Il conflitto di attribuzioni tra le Regioni e il potere giudiziario*, Giuffrè, Milano, 2001, 228 ss.

G. GRASSO, *La Corte costituzionale si pronuncia solo parzialmente sulla natura giuridica e sulla collocazione costituzionale delle Autorità indipendenti. Considerazioni sparse sulle decisioni n. 57, n. 118 e n. 226 del 1995*, in Quad. Reg., 1995, pag. 246.

A. P. GRIFFI, *Accesso incidentale alla Corte costituzionale e tutela dei diritti: note minime anche a proposito delle Authorities*, Intervento al convegno, organizzato da APro.M, dalle varie Associazioni nazionali dei magistrati, sia ordinari sia amministrativi, dal C.N.F. e dalla F.N.S.I. su Politica, Economia e Giustizia. La tutela dei diritti e delle libertà dei cittadini come fattori di garanzia, Tar Lazio, Sala Conferenze, 1 marzo 2006, consultabile su http://www.giustiziaamministrativa.it/documentazione/studi_contributi/Patroni_Griffi_Accesso_incidentaleallaCC.htm#_ftnref11.

E. GROSSO, *Autorità indipendente o autorità onnipotente? Il potere normativo di fatto del Garante per la protezione dei dati personali e il principio di legalità*, in M. G. LOSANO (a cura di), La legge italiana sulla privacy: un bilancio dei primi cinque anni, Laterza, 2001, pag. 140.

B. GUIDETTI SERRA, *Le schedature Fiat*, Rosenberg & Sellier, 1984.

E. JORIO, *La riforma sanitaria di Barack H. Obama*, in Federalismi.it, n. 17/2009, p. 1 ss., consultabile su http:www.federalismi.it.

M. KEYSER, *The Council of Europe Convention on Cybercrime*, consultabile su http://www.law.fsu.edu/Journals/ transnational/vol12_2/keyser.pdf.

C. LACAVA, in C.M. BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d.lgs. 30 giugno 2003, n. 196 (<<Codice della privacy>>)*, Cedam, Padova, pag. 1971.

E. LANDOLFI, *La giurisdizione ed Internet*, Diritto e diritti n.3/99.

G. LOMBARDO, *Le autorità amministrative indipendenti come poteri dello Stato nei conflitti di attribuzione*, in Quad. cost. 1998, pag. 290.

M G. LOSANO, *La legge spagnola sulla protezione dei dati personali*, in Il diritto dell'informazione e dell'informatica, 1993.

F.P. LUISO, *sub art 29*, in C.M. BIANCA, F.D. BUSNELLI, (a cura di), Tutela della privacy, in Nuove leggi civ., 1999, pag. 669 e ss.

J. LUTHER, R. ROMBOLI, R. TARCHI, *Esperienze di giustizia costituzionale*. Tomo I. Usa, Canada, Svizzera, Austria, Germania, Francia, Giappichelli, Torino, 2000.

F.P. LUISO, *Tutela amministrativa e giurisdizionale*, in F.D. BUSNELLI, (a cura di), Commento alla legge 31 dicembre 1996, n. 675, in Nuove leggi civ. comm., 1999, pag. 679.

D. LYON, *la società sorvegliata. Tecnologie di controllo della vita quotidiana*, con introduzione di S. RODOTà, Feltrinelli 2002.

E. MALFATTI, *Modelli e prassi di tutela dei diritti fondamentali, in Europa: un punto di vista italiano*, consultabile su http://joomla.ddp.unipi.it/documenti/persdoc/contributi/Elena%20Malfatti-1.pdf.

L. V. MANCINI, *L'era dell'ubiquitous computing*, in Innovazioni tecnologiche e privacy, consultabile su www.garanteprivacy.it.

A. MANEGGIA, *La tutela della privacy nell'era delle comunicazioni elettroniche: cosa ha cambiato Internet?*, in In.Law, 2006, pp. 303-323, consultabile su www.morlacchilibri.com/inlaw/downloads/in.law_08_3.pdf.

M. MANETTI, *I regolamenti delle autorità indipendenti*, in G. BRUNELLI, A. PUGIOTTO, P. VERONESI (a cura di), Scritti in onore di Lorenza Carlassare. Il diritto costituzionale come regola e limite al potere. Volume I , Delle fonti del diritto, Jovine, Napoli, 2009, p. 191. Consultabile su http://www.associazionedeicostituzionalisti.it/dottrina/fontidiritto/I%20Regolamenti%20delle%20Autorita%27%20indipendenti.pdf.

M. MANETTI, *Profili di giustizia costituzionale delle autorità indipendenti*, in Associazione italiana dei professori di diritto amministrativo, Annuario 2002, Giuffrè, Milano, 2003, pag 229. Anche in F. FRANCARIO (a cura di), Diritti, interessi ed amministrazioni indipendenti. Giornate di studio sulla giustizia amministrativa dedicate ad Eugenio Cannada Bartoli, Giuffrè, Milano, 2003, pag. 31 e ss.

S. MONTELEONE, *Dal controllo della tecnologia al controllo sulla tecnologia: necessità di un approccio tecnico giuridico*, consultabile su http://e-privacy.winstonsmith.info/2010/2007/atti/ep2007_Monteleone_controllo_tecnologia.pdf.

F. MANTOVANI, *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in AAVV, Il diritto alla riservatezza e la sua tutela penale, Atti del terzo simposio di studi di diritto e procedura penali, Varenna, Villa Monastero, 5-7 settembre 1967/ promosso dalla Fondazione "Avv. Angelo Luzzani" di Como - Giuffrè, Milano, 1970, pag 387.

S. MARASCIO, *le impronte digitali ed il sistema Afis*, in http://www.criminiseriali.it/AFIS.pdf.

P.C. MARCHISIO, *La valle dei geni*, in La Stampa del 30 marzo 2005.

T. MARTINES , *Diritto costituzionale*, Giuffrè Milano, 1997 pag 653.

V. F. MASCI, *Osservazioni critiche circa l'ammissibilità del diritto alla riservatezza*, in AAVV, Il diritto alla riservatezza e la sua tutela penale: Atti del terzo simposio di studi di diritto e procedura penali, Varenna, Villa Monastero, 5-7 settembre 1967/ promosso dalla Fondazione "Avv. Angelo Luzzani" di Como - Giuffrè, Milano, 1970, pp. 368 ss..

R. MASTROIANNI, *La tutela dei diritti fondamentali tra diritto comunitario e Costituzioni nazionali*, Relazione al Convegno della Corte di Cassazione "La tutela dei diritti fondamentali tra Corte costituzionale, Corti europee e giudice nazionale", Roma 21 gennaio 2009, consultabile su Osservatorio sul rispetto dei diritti fondamentali in Europa, www.europeanrights.eu, 2009, p. 17.

G. MATHIAS, *La legge <<Informatique et Libertés>>: un quadro giuridico rinnovato per la tutela dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Il codice del trattamento dei dati personali, Giappichelli, Torino, 2007. pag 923 e ss.

MATSUMOTO, H. MATSUMOTO, K. YAMADA, S. HOSHINO, *Impact of Artificial "Gummy" Fingers on Fingerprint Systems*, 2002, consultabile su http://cryptome.org/gummy.htm.

S. MELCHIONNA, in R. ACCIAI (a cura di), *Il diritto alla protezione dei dati personali: la disciplina sulla privacy alla luce del nuovo Codice*, Maggioli, Rimini, 2004, pag 70.

S. MELE, *Privacy e user generated content (UGC)*, in L BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, RCS Etas, Milano, 2010, pag 51 e ss.

S. MENTO, *Autorità indipendenti e rinvio pregiudiziale*, in Giornale di diritto amministrativo, n. 12/2005.

F. MERUSI, *Democrazia ed autorità indipendenti*, Mulino, 2000, pag. 27.

F. MERUSI, *le autorità indipendenti tra riformismo nazionale e autarchia comunitaria*, in F. A. GRASSINI (a cura di), L'indipendenza delle autorità, Il Mulino, Bologna, 2001, pagg. 26-27.

M. MEZZANOTTE, *il Diritto all'oblio vs diritto alla memoria: il moderno sviluppo della privacy*, in "Diritto pubblico comparato ed europeo", 2002.

B. MICOLANO, *Il diritto antidiscriminatorio nella giurisprudenza della Corte Europea dei diritti dell'uomo*, Giuffrè, Milano,2009, pag 277.

M. MIGLIAZZA, *Profili internazionali ed europei del diritto all'informazione e alla riservatezza*, Giuffè, Milano, 2004.

A. MILLER, *The assault of privacy*, an Arbor University of Michigan Press 1971.

A. R. MILLER, *Personal privacy in the computer age: The challenge of a new technology in an information-oriented society*, in Mich. L. Rev., 1969, 67, 1107.

F. MODUGNO, *Appunti dalle lezioni sulle fonti del diritto*, Giappichelli, 2002, pag. 78.

F. MODUGNO, *I "nuovi diritti" nella Giurisprudenza costituzionale*, Giappichelli, Torino, 1995, p. 107.

F. MODUGNO, *Riflessioni generali sulla razionalizzazione della legislazione e sulla delegificazione*, in Studi in onore di M. Mazziotti di Celso, Cedam, Padova 1995, pag. 206.

G. MORBIDELLI, *Sul regime amministrativo delle Autorità indipendenti*, in A. PREDIERI (a cura di), Le autorità indipendenti nei sistemi istituzionali ed economici, Passigli Editore, Firenze, 1997, Vol. I, pagg. 145 e ss.

V. NAPOLEONI, *I prelievi ematici coattivi dopo la sentenza della Corte costituzionale n. 238/1996. Prospettive di intervento normativo*, consultabile su http://www.ipzs.it/Pubblicazioni_ministeri/Min_giustizia/Documenti_giustizia/pdf/1996/10_1996/10_1996_2069-2082.pdf.

C. NARDELLI, *Il potere di nomina delle Autorità Indipendenti dei Presidenti di Camera e Senato della Repubblica italiana: un modello ormai superato*, consultabile su http://amministrazioneincammino.luiss.it/wpcontent/uploads/2010/04/15795_Nardelli.pdf.

B. NASCIMBENE e A. LANG, *Il Trattato di Lisbona: l'Unione europea a una svolta?*, in Il corriere giuridico, 2007.

D. NELKIN, *Informazione genetica: bioetica e legge*, in Riv. critica del diritto privato, 4/1994, p. 491.

S. NICCOLAI, *I Poteri garanti della Costituzione e le Autorità indipendenti*, ed. ETS, Pisa, 1996, pag 200.

S. NICCOLAI, *Quando nasce un potere.* In Giur. Cost, 1995, pag 1673 e ss.

S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006.

S. NIGER, *Privacy e tutela globale*, consultabile su http://www.diritto.it/materiali/informatica/niger2.html.

D. ONDEI, *Due licenze esegetiche: diritto alla riservatezza e diritto di cronaca*, Milano, 1965, pag 465.

A. PACE, *Le video registrazioni "ambientali" tra gli artt. 14 e 15 Cost*., in Giur. Cost.,. 2002, pag 1075.

A. PACE, *Problematica delle libertà costituzionali*, Cedam, Padova, 2003, III edizione, pag 20ss.

U. PAGALLO, *La tutela della Privacy negli Stati Uniti D'America e in Europa*, Giuffrè, Milano, 2008, pag 31.

L. PALAZZANI, *Introduzione alla biogiuridica*, Giappichelli, Torino, 2002, p. 97.

V. PAMIO, *Le novità introdotte dal Trattato di Lisbona. Spunti di riflessioni*, consultabile su http://www.giustamm.it/.

G.PAPI e F. RICCI, *La Telemedicina*, consultabile su http://www.uniroma2.it/didattica/fam/deposito/Telemedicina.pdf.

R. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali*, in R. PARDOLESI (a cura di), Diritto alla riservatezza e circolazione dei dati personali, Giuffrè, Milano, 2003, pag. 36.

A. PARISI, *Sicurezza informatica e tutela della privacy*, Istituto Poligrafico Zecca dello Stato S.p.a., 2006 pag. 113 e ss.

P. PASSAGLIA, *Il Trattato che adotta una costituzione per l'Europa. Due anni dopo*, Foro It., 2007, V, 19.

P. PASSAGLIA, *Il Trattato di Lisbona: qualche passo indietro per andare avanti*, in Il Foro It., 2008, n. 1, pp. 40-44.

S. PATTI, *Il consenso dell'interessato al trattamento dei dati personali*, in Rivista di diritto civile, 1999.

G. PEIETRI, *Biometria e riconoscimento biometrico della persona*, consultabile su http://85.94.202.75/ sistemadocumentale/AreaDocumenti/E.../Biometria.doc.

P. PERLINGIERI, *La personalità umana nell'ordinamento giuridico.* Camerino-Napoli, 1972.

P. PERRI, *Privacy, diritto e sicurezza informatica,* Giuffrè, Milano 2007, pag. 195 e ss.

A. PERTICI, *Il Trattato costituzionale nel processo di costituzionalizzazione europea*, consultabile su www.unipi.it/athenet1-14/13/articoli/0013Pertici_boxA.html.

M. PETRONE, *Trattamento di dati genetici e tutela della persona*, in Fam. e dir., 8-9/2007, p. 853 ss.

F. PICCALUGA, *L'inadeguatezza del modello camerale alla luce del novellato art. 111 cost.* - nota ad App. Genova, ord. 4 gennaio 2001, In Giust. Civ., 2002, Vol. 52 c. 1383.

C. PICIOCCHI, *La Convenzione di Oviedo sui diritti dell'uomo e della biomedicina: verso una bioetica europea?*, in Diritto pubblico comparato ed europeo, 2001, III, p. 1301 ss.

N. PIGNATELLI, *Sulla natura del ricorso straordinario: l'illegittimità costituzionale dell'art. 69 della l. 69/2009*, consultabile su http://www.forumcostituzionale.it/site/images/stories/pdf/documenti_forum/temi_attualita/_presidente_repubblica/0003_pignatelli.pdf.

N. PIGNATELLI, *Sulla " natura" del ricorso straordinario: la scelta del legislatore (art. 69 l. 69/2009)*, in Rivista Neldiritto, Speciale. Le nuove norme su procedimento e processo amministrativo. Commento alle novità introdotte dalla legge 18 giugno 2009, n. 69, consultabile su http://www.giustizia-amministrativa.it/documentazione/studi_contributi/2009_7_Pignatelli_Le_scelte_del_legislatore.htm.

R. PINARDI (a cura di) *Le zone d'ombra della giustizia costituzionale. I giudizi sui conflitti di attribuzione e sull'ammissibilità del referendum abrogativo*, Atti del seminario di Modena, 13 ottobre 2006, Giappichelli, Torino, 2007.

R. PINARDI, *Quando l'arbitro diventa portiere (della Corte): notazioni minime sulla "naturale" elasticità della nozione di giudice a quo*, in Giur. Cost., 2001, 3756.

G. PINO, *conflitto e bilanciamento fra diritti individuali. Una mappa dei problemi*, consultabile su http://www.unipa.it/gpino/Conflitto%20e%20bilanciamento.pdf.

F. PIZZETTI, *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, in P. BILANCIA e M. D'AMICO (a cura di) La nuova Europa dopo il Trattato di Lisbona, Giuffrè, Milano, 2009.

F. PIZZETTI, *Sicurezza, privacy, efficienza dei servizi: come conciliare i diritti per lo sviluppo di una moderna pubblica amministrazione*, Roma, 22 novembre 2007, consultabile su http://www.forumpa.it/convegni/sicurezzaprivacy/documenti/Pizzetti.pdf.

A. PIZZORUSSO, *La Costituzione. I valori da conservare, le regole da cambiare*, Einaudi, Torino, 1996.

A. PIZZORUSSO, *Lezioni di diritto costituzionale*, Il Foro italiano, Roma, 1978 e 1984.

A. PIZZORUSSO, *Sul diritto alla riservatezza nella Costituzione italiana*, in Prassi e Teoria, 1976, p. 37.

F. POLITI, *La potestà amministrativa delle Autorità amministrative indipendenti: nuovi profili di studio*, in N. LONGOBARDI, Autorità amministrative indipendenti e sistema giuridico-istituzionale, 2° ed, Giappichelli, Torino, 2009, pag 298.

F. PORCIANI, *Chi protegge il Dna degli italiani*, in Il Corriere della Sera, 23 maggio 2004, consultabile su http://archiviostorico.corriere.it/2004/maggio/23/Chi_protegge_Dna_degli_italiani_cs_0_040523156.shtml.

P. POZZANI, *Nuovi profili del diritto di accesso dopo la L.15/05*, consultabile su http://www.giustizia-amministrativa.it/documentazione/20050913Pozzani.htm.

A. PREDIERI, *L'erompere delle autorità amministrative indipendenti*, Passigli,1997.

F. S. PROFITI, *Lo stato di attuazione dell'E-Goverment in Italia*, consultabile su http://www.cattolici-liberali.com/tocquevilleacton/pubblicazioni/focus/focus-paper20_ottobre08.pdf.

M. PROSPERI, *Il diritto alla riservatezza nell'ordinamento costituzionale*, consultabile su http://www.dirittoproarte.com/dirarti/costituzione.htm.

M. PROSPERI, *Il dibattito italiano sull'esistenza e sul fondamento del diritto alla riservatezza prima del suo espresso riconoscimento*, consultabile su http://www.privacy.it/prosperi200206.html.

W. PROSSER, *Privacy*, in Cal. L. Rev., 1960, 48, 383.

G. PUGLIESE, *Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche*, nota a Trib. Roma, 14 settembre 1953, in Foro it., 1954, I, 116.

A PUNZI, *La persona nei dati. Ragioni e modelli di una regolamentazione*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Il codice del trattamento dei dati personali, Giappichelli, Torino, 2007.

G. QUACQUARELLI, *La Convenzione sulla biomedicina del Consiglio d'Europa*, in Riv. dir. pubbl. e Scienza politica, 1997, p. 265 ss.

M. QUATRARO, *Body scanner negli aeroporti in Italia:paura per la salute. Privacy a rischio con immagine spedite?*, articolo consultabile su http://www.businessonline.it/news/9719/Body-scanner-negli-aeroporti-in-Italia-paura-per-la-salute-privacy-a-rischio-con immagine-spedite.html.

F. RAIA, *Privacy e diritto di cronaca con riguardo a particolari categorie di soggetti: le persone pubbliche e i minori*, consultabile su http://www.associazionedeicostituzionalisti.it/dottrina/libertadiritti/raia.html.

G. RASI, *Cosa cambiare per le attività produttive*, in G. RASI (a cura di), Privacy: da costo a risorsa, consultabile su www.garanteprivacy.it.

G. RASI, *Progresso tecnologico e sviluppo civile*, in Innovazioni tecnologiche e privacy, consultabile su www.garanteprivacy.it.

G. RASI, Convegno: "La sicurezza partecipata: coordinamento e cooperazione interistituzionale", Forum P.A. 2004, http://www.garanteprivacy.it/garante/doc.jsp?ID=1001758.

S. REGASTO, *Contributo allo studio delle Autorità Indipendenti. Il caso del garante per l'editoria e la radiodiffusione*, ARACNE editrice S.r.l., 2004.

G. RESTA, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in Rivista critica del diritto privato, pp. 310 e ss.

G. U. RESCIGNO, *Sul principio di legalità*, in Diritto pubblico, 1995, 247, ss.

V. RICCIUTO, *Le Finalità del Codice*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Il codice del trattamento dei dati personali, Giappichelli, Torino, 2007.

P. RIDOLA, *Libertà e diritti nello sviluppo storico del costituzionalismo*, in P. RIDOLA, R. NANIA (a cura di), I diritti costituzionali, II ed., Giappichelli,Torino, 2006, vol. I, pag. 143.

P. RIDOLFI, *Amministrazione digitale. Compendio normativo*, Collana Minigrafie, Tecnologia dei processi documentali, Fondazione Siav Academy, 2010, consultabile sul sito www.digita-lex.it.

P. RIDOLFI (a cura di), *Il nuovo Codice della Amministrazione Digitale*, Collana di Minigrafie, Tecnologia dei Processi Documentali, 2011 Fondazione Siav Academy - Edizione fuori commercio, consultabile sul sito http://www.digita-lex.it/pages/documents/ita/minigrafia7.pdf.

S. RODOTà, *Apologia dei diritti*, in Lezioni Noberto Bobbio, Torino 2004, consultabile su http://www.scribd.com/doc/53206551/Apologia-dei-diritti-Stefano-Rodota-I-diritti-dell-uomo-oggi-Norberto-Bobbio.

S. RODOTà, *Diritto, scienza e tecnologia: modelli e scelte di regolamentazione*, in Riv. cri. dir. priv., a. XXII, n. 3, sett. 2004, p.372.

S. RODOTà *Elaboratori elettronici e controllo sociale*, il Mulino, Bologna,1973.

S.RODOTà, *Relazione introduttiva al Convegno "Internet e privacy - quali regole?"*, Roma 8-9 maggio 1998, consultabile su http://www.interlex.it/675/rodotint.htm e http://www.privacy.it/garanterelrod.html per gli altri atti del Convengo si veda http://www.privacy.it/garante1998convegno.html.

S. RODOTà, *Internet tra sicurezza e normalizzazione*, La Repubblica 15-1-2009, consultabile su http://www.astrid-online.it/Forme-e-st/Rassegna-s/LA-REPUBBLICA_S_Rodot--15_01_09.pdf.

S. RODOTà, *Internet Bill of rights: nuovi diritti che vanno condivisi e riconosciuti*, consultabile su http://saperi.forumpa.it/story/33743/internet-bill-rights-nuovi-diritti-che-vanno-condivisi-e-riconosciuti.

S. RODOTà *Internet è un diritto, va scritto in Costituzione*, consultabile su http://mag.wired.it/rivista/storie/stefano-rodota-internet-e-un-diritto-che-va-scritto-nellacostituzione.html.

S. RODOTà, *Intervista su privacy e libertà*, a cura di P. Conti, Editori Laterza 2005.

S. RODOTà, *Laicizzare il rapporto fra innovazione e società*, in Innovazioni tecnologiche e privacy, consultabile su www.garanteprivacy.it.

S. RODOTà, *Libertà personale. Vecchi e nuovi nemici*, in M. BOVERO (a curadi), Quale libertà. Dizionario contro i falsi liberali, Laterza, Roma-Bari, 2004, pag 52.

S. RODOTà, *L'ansia di sicurezza che cancella i diritti*, consultabile su http://www.privacy.it/rodo20011023.htm.l

S. RODOTà, *La vita e le regole. Tra diritto e non diritto*, Feltrinelli, 2006.

S. RODOTà, *La <<privacy>> tra individuo e collettività*, Pol. dir., Il Mulino, Bologna,1974, pag. 545.

S. RODOTà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in Rivista critica di diritto privato, 1997, pag 595.

S. RODOTà, *Quel conflitto tra pivacy e sicurezza*, consultabile su http://www.privacy.it/rodo20020610.html.

S. RODOTà, *Tra i diritti fondamentali ed elasticità della normativa: il nuovo codice della privacy*, Eur.dir. priv., 2004, 2.

S. RODOTà, *Tecnologia e diritti*, Il Mulino, Bologna, 1995, pag 19.

S. RODOTà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazioni*, Laterza, Roma-Bari 1997.

S. RODOTà, *Tra diritti fondamentali ed elasticità della normativa:il nuovo Codice della privacy*, in Europa e diritto privato, 2004, fasc. 1, pp. 1-10.

S. RODOTà, *Una Carta dei diritti del web*, consultabile su http://www.repubblica.it/2007/11/sezioni/ scienza_e_tecnologia/rodota-web/rodota-web/rodota-web.html.

G. ROLLA, *Il difficile equilibrio tra diritti di informazione e tutela della dignità e della vita privata: brevi considerazioni alla luce dell'esperienza italiana*, consultabile su www.unisi.it/ricerca/dip/dir_eco/COMPARATO/rolla4.doc.

G ROLLA, *Le prospettive dei diritti della persona alla luce delle recenti tendenze costituzionali*, in "Quaderni costituzionali", 1997.

G ROLLA (a cura di), *Tecniche di garanzia dei diritti fondamentali*, Giappichelli, Torino, 2001.

R. ROMBOLI, *Corte e Diritti*, in Corte costituzionale e sistema istituzionale, Convegno dell'Associazione Gruppo di Pisa, (Pisa 4-5 giugno 2010), in corso di pubblicazione in Quaderni del Gruppo di Pisa, Giappichelli, Torino, 2011.

R. ROMBOLI, *Una sentenza "storica": la dichiarazione di incostituzionalità di un decreto-legge per evidente mancanza dei presupposti di necessità e di urgenza*, in Il Foro italiano, 2007, fasc. 7/8,

consultabile su http://www.associazionedeicostituzionalisti.it/giurisprudenza/decisioni2/romboli/nota171_2007.html.

R. ROMBOLI (a cura di), *Aggiornamenti in tema di processo costituzionale (2005-2007)*, Giappichelli, 2008.

R. ROMBOLI, *Il significato essenziale della motivazione per le decisioni della Corte costituzionale in tema di diritti di libertà pronunciate a seguito di bilanciamento tra valori costituzionali contrapposti*, in V. ANGIOLINI (a cura di), Libertà e giurisprudenza costituzionale, Giappichelli, Torino, 1992, pp. 206-220.

R. ROMBOLI, *La relatività dei valori costituzionali per gli atti di disposizione del proprio corpo*, in Pol. del dir., 1991, pag 565 ss.

R. ROMBOLI, *Per la Corte costituzionale le coppie omosessuali sono formazioni sociali, ma non possono accedere al matrimonio*, in Foro It., 2010, I, 1367.

R. ROMBOLI, *Il diritto "consentito" al matrimonio ed il diritto "garantito" alla vita familiare per le coppie omosessuali in una pronuncia in cui la Corte dice "troppo" e "troppo poco"*, in Giur. cost., 2010, fasc. 2.

R. ROMBOLI, E. MALFATTI, S. PANIZZA, *Giustizia costituzionale*, Giappichelli, Torino, 2007.

E. ROSO ACUNA, *Habeas Data costituzionale: nuova garanzia giurisdizionale del diritto pubblico latinoamericano*, in Dir. Pubb. Comparato ed europeo, n 4 2002, 1923.

S. ROSSI, *Body Scanner*, articolo pubblicato il 31 dicembre 2009 su http://it.reuters.com/article/ topNews/idITMIE5BU0BT20091231.

M. RUOTOLO, *La sicurezza nel gioco del bilanciamento*, Testo della relazione presentata al Convegno "I diversi volti della sicurezza", svoltosi presso l'Università degli Studi di Milano – Bicocca il 4 giugno 2009, consultabile su http://www.associazionedeicostituzionalisti.it/dottrina/libertadiritti/ruotolo_la%20sicurezza%20nel%20gioco%20del%20bilanciamento.pdf.

G.M. SALERNO, *I profili soggettivi nei conflitti di attribuzione relativi alla par condicio*, in F. MODUGNO (a cura di), Par condicio *e Costituzione*, Giuffrè, Milano, 1997, pag. 19 e ss.

P. SAMUELSON, *Privacy as intellectual property?*, in Stan . L. Rev., 2000.

E. SANCHEZ JIMENEZ, *los derechos humanos de la tercera generatiòn: la libertad informatica*, (Comunicazione presentata al III Congresso Iberoamericano di Informatica e diritto) in Informatica y Derecho, n 3, 1992, 85 e ss.

M. A. SANDULLI, *Accesso alle notizie e ai documenti amministrativi (sub voce)*, in Enc. Dir., IV, Aggiorn., Milano 2000, p. 19.

M. A. SANDULLI, *Il Procedimento*, in S. CASSESE (a cura di), *Trattato di diritto amministrativo*, Tomo II, Guffrè, Milano, 2003, p. 1165.

G. SANTANIELLO, *I codici di deontologia nel trattamento dei dati personali*, in www.interlex.it del 24 ottobre 2002.

G. SANTANIELLO, *Tipologia delle innovazioni tecnologiche e protezione dei dati personali*, in Innovazione tecnologiche e privacy, consultabile su www.garanteprivacy.it.

G. SANTANIELLO, C. FILIPPI, *Dati genetici, genoma e privacy*, in A. LOIODICE, G. SANTANIELLO (a cura di), La tutela della riservatezza, Trattato di diritto amministrativo diretto da G. Santaniello, Cedam, Padova, 2000, pp. 521-526

C. SARTORETTI, *Contributo allo studio del diritto alla privacy nell'ordinamento costituzionale. Riflessioni sul modello francese*, Giappichelli, Torino, 2008, pag. 47.

F. SATTA, *La riforma della legge 241/90: dubbi e perplessità*, in www.giustamm.it, Speciale sulla riforma della L.241/1990.

M. SAVASTANO, *Recenti applicazioni biometriche*, in Innovazioni tecnologiche e privacy, consultabile su www.garanteprivacy.it.

C. SBAILO', *Trattato di Prüm, una rivoluzione silenziosa (finora)*, consultabile su http://www.forumcostituzionale.it/site/images/stories/pdf/documenti_forum/temi_attualita/guerra_terrorismo/0001_sbailo.pdf.

L. SCAFFARDI, *Le banche dati genetiche per fini giudiziari e la libertà della persona*, in C. CASONATO C. PICIOCCHI P. VERONESI (a cura di), Forum biodiritto 2008. La circolazione dei modelli nel biodiritto, Cedam, Padova, 2009 consultabile su http://www.forumcostituzionale.it/site/images/stories/pdf/documenti_forum/paper/0114_scaffardi.pdf.

F. A. SCHURR, *La tutela dei dati personali nell'esperienza tedesca*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Il codice del trattamento dei dati personali, Giappichelli, Torino, 2007. pag 975 e ss.

C. SILVESTRO, *E-government, e-governance, edemocracy*, in G. CASSANO (a cura di), Diritto delle nuove tecnologie informatiche e dell'Internet, IPSOA 2002, pag. 1279-1281.

G. SIRIANI, *Nuove tendenze legislative in materia di amministrazioni indipendenti*, Nomos, 1993, pag. 89 e ss.

F. SORRENTINO, *Sulle fonti del diritto*, ed. E.C.I.G., Genova 2002, pag. 143.

R. STAGLIANO, *Silenzio, il cellulare ti spia. Se il telefonino diventa nemico*, La Repubblica, 2 luglio 2009, consultabile su http://www.repubblica.it/2009/07/sezioni/tecnologia/privacy-telefoni/privacy-telefoni/privacy-telefoni.html.

S. STAMMATI, *Tre questioni in materia di "autorità amministrative indipendenti"*, in Associazione Italiana dei Costituzionalisti, Autorità indipendenti e principi costituzionali, Cedam, Padova, 1999, pag. 84.

E. STEFANINI, *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, Cedam, Padova, 2008, p. 90.

S. STIZIA, *Informazione, nuove tecnologie e cambiamenti relazionali tra PA e cittadini*, in Diritto dell'Internet, Ipsoa, n.6/2006, p.615.

M. SURACE, *Evoluzione storico-giuridica del diritto alla riservatezza: da diritto borghese a sinonimo di libertà*, in Analisi socio-giuridica del rapporto tra sorveglianza e diritto alla riservatezza nell'era di Internet, cap 2, consultabile su http://www.altrodiritto.unifi.it/ricerche/control/surace/cap2.htm.

D. TEGA, *Le sentenze della Corte costituzionale nn. 348 e 349 del 2007: la Cedu da fonte ordinaria a fonte "sub-costituzionale" del diritto*, consultabile in http://www.forumcostituzionale.it/site/images/stories/pdf/documenti_forum/giurisprudenza/2007/0013_tega_nota_348_349_2007.pdf.

G. TIBERI, *Riservatezza e protezione dei dati personali*, in M. CARTABIA (a cura di), I diritti in azione, Universalità e pluralismo dei diritti fondamentali nelle Corti europee, Il Mulino, 2007, pag 351.

R. TOMMASSINI, *Osservazioni in tema di diritto alla privacy*, in Dir. Famiglia, 1976, pag. 255.

P. TORRETTA, *Privacy e nuove forma di discriminazione rispetto alla circolazione delle informazioni genetiche:sistemi giuridici di tutela a confronto*, consultabile su www.associazionedeicostituzionalisti.it/dottrina/libertadiritti/Torretta.pdf.

E. TRAVERSA e G. D'ANGELO, *Diritto tributario e privacy: un binomio critico*, in L BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), Next Privacy, RCS Etas, Milano, 2010, pag 229 e sgg.

P. TROIANO, *Le misure di sicurezza*, in G. SANTANIELLO (a cura di), La protezione dei dati personali, Cedam, Padova, 2005, pag. 209 e ss.

T. M. UBERTAZZI, *Diritto alla privacy, natura e funzioni giuridiche*, Cedam, Padova, 2004, pag 76.

F. VATALARO, *Privacy e sicurezza in ambito wireless*, Convegno"Innovazioni tecnologiche e privacy. Sviluppo economico e progresso civile ", Roma 17-18 giugno 2004, pag 166 consultabile su http://www.garanteprivacy.it/garante/document?ID=1595454.

P. VERONESI, *Recenti tendenze in materia di conflitti di attribuzioni fra poteri. Profili soggettivi e oggettivi*, in Ann. Univ. Ferrara- Sc. Giur., Nuova serie, V. XVI (2002), consultabile su http://web.unife.it/progetti/annuali/scienze_giuridiche/2002/pdf/06.pdf.

G. VETTORI, *Carta europea e diritti dei privati*, Cedam, Padova, 2002.

I. WALDEN, *Data protection nel Regno Unito*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Il codice del trattamento dei dati personali, Giappichelli, Torino, pag. 992 e ss.

S.WARREN, L.D.BRANDEIS, *The right of privacy*, in Harv. L. Rev., 1890, 4, 193.

A. F. WESTIN, *Privacy and Freedom*, Atheneum, New York, 1967, pag. 1.

M. WINKLER, *La giurisdizione nel ciberspazio*, in Ciberspazio e Diritto, Volume II, Numero II, pp. 197-240. Articolo tratto dal sito http://www.ciberspazioediritto.org.

G. ZICCARDI, *La libertà di espressione inInternet al vaglio della Corte Suprema degli Stati Uniti*, in Quaderni costituzionali, n.1, 1998, 123 ss.

J. ZILLER, *Il nuovo Trattato europeo*, Il Mulino,Bologna, 2007.

P. ZIVIZ, *Trattamento dei dati personali e responsabilità civile: il regime previsto dalla legge 675*, in Responsabilità civile e previdenza, 1997.